So IP1376 US00

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　９月　１日

出願番号
Application Number: 特願２０００－２６４９２３

出願人
Applicant(s): ソニー株式会社

２００１年　６月２８日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０６０８５９

【書類名】　特許願

【整理番号】　0000508204

【提出日】　平成12年 9月 1日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/00

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　山田　真

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　鵜飼　伸光

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　佐藤　順一

【発明者】

【住所又は居所】　東京都港区南青山１丁目１番１号　株式会社ソニーファイナンスインターナショナル内

【氏名】　川合　成幸

【発明者】

【住所又は居所】　東京都港区南青山１丁目１番１号　株式会社ソニーファイナンスインターナショナル内

【氏名】　奥出　勉

【発明者】

【住所又は居所】　東京都港区南青山１丁目１番１号　株式会社ソニーファイナンスインターナショナル内

【氏名】　伊藤　浩二

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100082131

【弁理士】

【氏名又は名称】　稲本　義雄

【電話番号】　03-3369-6479

【手数料の表示】

【予納台帳番号】　032089

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9708842

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置、および情報処理方法、電子マネーサービス提供システム、並びに記録媒体

【特許請求の範囲】

【請求項１】　電子マネーサービスにおける電子マネーブランドの管理、並びに、前記電子マネーサービスの提携事業者の開拓および管理を行う第１の事業者が管理する情報処理装置において、

電子マネー情報、および前記電子マネーサービスに関する認証処理に用いられる認証情報が記録される第１の情報処理装置を発行する第２の事業者が管理する第２の情報処理装置と情報を授受する第１の授受手段と、

前記電子マネーを利用したサービスを提供する第３の事業者が管理する第３の情報処理装置と情報を授受する第２の授受手段と、

前記電子マネーサービスに関する認証処理に用いられる前記認証情報を記録する第１の記録手段と、

前記第２の事業者に関する情報、および前記第１の事業者と前記第２の事業者との提携内容に関する情報を記録する第２の記録手段と、

前記第３の事業者に関する情報、および前記第１の事業者と前記第３の事業者との提携内容に関する情報を記録する第３の記録手段と

を備え、

前記第１の授受手段は、前記第２の記録手段により記録された前記第１の事業者と前記第２の事業者との提携内容に関する情報に基づいて、前記第１の記録手段により記録された前記認証情報を出力し、

前記第２の授受手段は、前記第３の記録手段により記録された前記第１の事業者と前記第３の事業者との提携内容に関する情報に基づいて、前記第１の記録手段により記録された前記認証情報を出力する

ことを特徴とする情報処理装置。

【請求項２】　前記認証情報は、ＤＥＳを適応した秘密鍵情報を含む

ことを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記第２の事業者との課金処理を実行する第１の課金手段と、

前記第３の事業者との課金処理を実行する第２の課金手段と

を更に備えることを特徴とする請求項１に記載の情報処理装置。

【請求項４】　前記第１の記録手段により記録された前記認証情報を用いた認証処理を実行する認証手段を更に備え、

前記認証手段は、前記第２の授受手段により、前記第３の事業者より認証処理の実行を要求する信号が入力された場合、前記第１の記録手段により記録された前記第３の事業者に対応する前記認証情報を用いて認証処理を実行する

ことを特徴とする請求項１に記載の情報処理装置。

【請求項５】　前記第１の情報処理装置に記録された前記電子マネー情報を書き換える処理を行う第４の情報処理装置と、ネットワークを介して情報を授受する第３の授受手段と、

前記第４の情報処理装置に、前記第１の情報処理装置に対する前記電子マネーの充填処理を実行させるための制御信号を生成する生成手段と

を更に備え、

前記生成手段は、前記第２の記録手段により記録された、前記第１の事業者と前記第２の事業者との提携内容に関する情報に基づいて、前記第２の事業者が発行した前記第１の情報処理装置に対する前記制御信号を生成し、

前記第３の授受手段は、前記生成手段により生成された前記制御信号を、前記第４の情報処理装置へ出力する

ことを特徴とする請求項１に記載の情報処理装置。

【請求項６】　前記ネットワークは、インターネットであり、

前記第３の授受手段は、更に、前記インターネット上に仮想店舗を有する前記第３の事業者が管理する第５の情報処理装置と情報を授受する

ことを特徴とする請求項７に記載の情報処理装置。

【請求項７】　電子マネーサービスにおける電子マネーブランドの管理、並びに、前記電子マネーサービスの提携事業者の開拓および管理を行う第１の事業者が管理する情報処理装置の情報処理方法において、

電子マネー情報、および前記電子マネーサービスに関する認証処理に用いられる認証情報が記録される第１の情報処理装置を発行する第２の事業者が管理する

第２の情報処理装置と情報を授受する第１の授受ステップと、

前記電子マネーを利用したサービスを提供する第３の事業者が管理する第３の情報処理装置と情報を授受する第２の授受ステップと、

前記電子マネーサービスに関する認証処理に用いられる前記認証情報を記録する第１の記録ステップと、

前記第２の事業者に関する情報、および前記第１の事業者と前記第２の事業者との提携内容に関する情報を記録する第２の記録ステップと、

前記第３の事業者に関する情報、および前記第１の事業者と前記第３の事業者との提携内容に関する情報を記録する第３の記録ステップと

を含み、

前記第１の授受ステップの処理では、前記第２の記録ステップの処理により記録された前記第１の事業者と前記第２の事業者との提携内容に関する情報に基づいて、前記第１の記録ステップの処理により記録された前記認証情報を出力し、

前記第２の授受ステップの処理では、前記第３の記録ステップの処理により記録された前記第１の事業者と前記第３の事業者との提携内容に関する情報に基づいて、前記第１の記録ステップの処理により記録された前記認証情報を出力する

ことを特徴とする情報処理方法。

【請求項８】　電子マネーサービスにおける電子マネーブランドの管理、並びに、前記電子マネーサービスの提携事業者の開拓および管理を行う第１の事業者が管理する情報処理装置用のプログラムであって、

電子マネー情報、および前記電子マネーサービスに関する認証処理に用いられる認証情報が記録される第１の情報処理装置を発行する第２の事業者が管理する第２の情報処理装置と情報を授受する第１の授受ステップと、

前記電子マネーを利用したサービスを提供する第３の事業者が管理する第３の情報処理装置と情報を授受する第２の授受ステップと、

前記電子マネーサービスに関する認証処理に用いられる前記認証情報を記録する第１の記録ステップと、

前記第２の事業者に関する情報、および前記第１の事業者と前記第２の事業者との提携内容に関する情報を記録する第２の記録ステップと、

前記第３の事業者に関する情報、および前記第１の事業者と前記第３の事業者との提携内容に関する情報を記録する第３の記録ステップと

を含み、

前記第１の授受ステップの処理では、前記第２の記録ステップの処理により記録された前記第１の事業者と前記第２の事業者との提携内容に関する情報に基づいて、前記第１の記録ステップの処理により記録された前記認証情報を出力し、

前記第２の授受ステップの処理では、前記第３の記録ステップの処理により記録された前記第１の事業者と前記第３の事業者との提携内容に関する情報に基づいて、前記第１の記録ステップの処理により記録された前記認証情報を出力する

ことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項９】　電子マネーサービスにおける電子マネーブランドの管理、並びに、前記電子マネーサービスの提携事業者の開拓および管理を行う第１の事業者が管理する第１の情報処理装置と、

電子マネー情報、および前記電子マネーサービスに関する認証処理に用いられる認証情報が記録される第２の情報処理装置と、

前記第２の情報処理装置を発行する第２の事業者が管理する第３の情報処理装置と、

前記電子マネーを利用したサービスを提供する第３の事業者が管理する第４の情報処理装置と

からなる電子マネーサービス提供システムにおいて、

前記第１の情報処理装置は、

前記第２の事業者が管理する第３の情報処理装置と情報を授受する第１の授受手段と、

前記第３の事業者が管理する第４の情報処理装置と情報を授受する第２の授受手段と、

前記電子マネーサービスに関する認証処理に用いられる前記認証情報を記録する第１の記録手段と、

前記第２の事業者に関する情報、および前記第１の事業者と前記第２の事業

者との提携内容に関する情報を記録する第２の記録手段と、
前記第３の事業者に関する情報、および前記第１の事業者と前記第３の事業者との提携内容に関する情報を記録する第３の記録手段と
を備え、
前記第１の授受手段は、前記第２の記録手段により記録された前記第１の事業者と前記第２の事業者との提携内容に関する情報に基づいて、前記第１の記録手段により記録された前記認証情報を出力し、
前記第２の授受手段は、前記第３の記録手段により記録された前記第１の事業者と前記第３の事業者との提携内容に関する情報に基づいて、前記第１の記録手段により記録された前記認証情報を出力し、
前記第２の情報処理装置は、
前記第１の授受手段によって、前記第３の情報処理装置へ出力された前記認証情報を記録する第４の記録手段と、
前記電子マネー情報を記録する第５の記録手段と
を備え、
前記第３の情報処理装置は、
前記第１の情報処理装置と情報を授受する第３の授受手段と、
前記第３の授受手段により入力された前記認証情報を記録する第６の記録手段と、
前記第２の情報処理装置の発行に関する情報を記録する第７の記録手段と、
前記第６の記録手段により記録された前記認証情報に基づいて、前記第２の情報処理装置との認証処理を実行する第１の認証処理実行手段と
を備え、
前記第４の情報処理装置は、
前記第１の情報処理装置と情報を授受する第４の授受手段と、
前記第４の授受手段により入力された前記認証情報を記録する第８の記録手段と、
前記第８の記録手段により記録された前記認証情報に基づいて、前記第２の情報処理装置との認証処理を実行する第２の認証処理実行手段と

を備える

ことを特徴とする電子マネーサービス提供システム。

【請求項１０】　前記第３の情報処理装置は、

前記第２の情報処理装置の前記第５の記録手段により記録された前記電子マネー情報を書き換える処理を実行する複数の第５の情報処理装置と情報を授受する第５の授受手段を更に備え、

前記第１の認証手段は、前記第５の授受手段により入力された、前記第２の情報処理装置の前記第４の記録手段により記録された前記認証情報に基づいて認証処理を実行する

ことを特徴とする請求項９に記載の電子マネーサービスシステム。

【請求項１１】　前記第４の情報処理装置は、

前記第２の情報処理装置の前記第５の記録手段により記録された前記電子マネー情報を書き換える処理を実行する複数の第５の情報処理装置と情報を授受する第５の授受手段を更に備え、

前記第２の認証手段は、前記第５の授受手段により入力された、前記第２の情報処理装置の前記第４の記録手段により記録された前記認証情報に基づいて認証処理を実行する

ことを特徴とする請求項９に記載の電子マネーサービスシステム。

【請求項１２】　前記第４の情報処理装置は、

前記第２の情報処理装置と情報を授受する第５の授受手段と、

前記第２の情報処理装置の前記第５の記録手段により記録された前記電子マネー情報を書き換えさせるための制御信号を生成する生成手段と

を更に備え、

前記第２の認証手段は、前記第５の授受手段により入力された、前記第２の情報処理装置の前記第４の記録手段により記録された前記認証情報に基づいて認証処理を実行する

ことを特徴とする請求項９に記載の電子マネーサービスシステム。

【請求項１３】　前記第２の情報処理装置は、

個人認証カード、入退出鍵、定期券、ポイントカード、会員カード、キャッシ

ュカード、クレジットカード、もしくはローンカードのうち、少なくとも一つの機能を実行するアプリケーションを記録する第９の記録手段を更に備える

ことを特徴とする請求項９に記載の電子マネーサービス提供システム。

【請求項１４】　前記第２の情報処理装置は、非接触型ＩＣカードである

ことを特徴とする請求項９に記載の電子マネーサービス提供システム。

【請求項１５】　前記第２の情報処理装置は、接触型ＩＣカードである

ことを特徴とする請求項９に記載の電子マネーサービス提供システム。

【請求項１６】　前記第２の情報処理装置は、携帯電話機である

ことを特徴とする請求項９に記載の電子マネーサービス提供システム。

【請求項１７】　前記第２の情報処理装置は、ＰＤＡである

ことを特徴とする請求項９に記載の電子マネーサービス提供システム。

【請求項１８】　前記第２の情報処理装置は、パーソナルコンピュータである

ことを特徴とする請求項９に記載の電子マネーサービス提供システム。

【請求項１９】　前記第２の情報処理装置は、時計である

ことを特徴とする請求項９に記載の電子マネーサービス提供システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置、および情報処理方法、電子マネーサービス提供システム、並びに記録媒体に関し、特に、電子マネー事業において、１つのブランドに対して、多くのイシュアおよび加盟店が参画することができ、イシュアおよび加盟店に対する暗号鍵の配布、およびシステムの運営・管理に必要となるコストを低減することができる、情報処理装置、および情報処理方法、電子マネーサービス提供システム、並びに記録媒体に関する。

【０００２】

【従来の技術】

電子マネーシステムや、セキュリティシステムにおいて、ＩＣ（Integrated circuit）カードの利用が増加している。ＩＣカードとは、ＩＣチップが埋め込まれたカード状デバイスのことであり、例えば、各種処理を行うＣＰＵ（Central

Processing Unit）などの演算処理部や、処理に必要なデータなどを記憶するメモリなどを内蔵している。ＩＣカードは、所定のリーダ／ライタを利用して、電気的に接触させた状態、もしくは、電磁波を利用した非接触の状態で、データの読み書きが行われる。

【０００３】

また、ＩＣカードを、電子マネーシステムやセキュリティシステムなどで利用する場合においては、データの隠匿性や、ＩＣカードの偽造を防止すること等のセキュリティが重要であり、データの記憶のためのリソース管理や、データに対するフレキシブルでセキュリティの高いアクセス制御を行うことが必要である。

【０００４】

ＩＣカードを用いた電子マネー事業は、電子マネーのブランドを管理するブランドホルダ、電子マネー事業における加盟店を開拓したり、管理するアクワイアラ、およびＩＣカードを発行するイシュアの３つの機能により構築されている。

【０００５】

従来、電子マネー事業は、ブランドホルダ、アクワイアラ、およびイシュアの３つの機能を一元的に行う事業体により行われているか、もしくは、それぞれのドメインを独立させ、1つのブランドホルダに対して、複数のアクワイアラおよび複数のイシュアが提携することにより行われてきた。

【０００６】

【発明が解決しようとする課題】

しかしながら、ブランドホルダ、アクワイアラ、およびイシュアの３つの機能を一元的に有する１つの事業体により、電子マネー事業が行われる場合、その事業体は、電子マネー事業運営のためのシステム投資、加盟店用の端末装置などのハードウェアリソース、ＩＣカードの発行および管理コストなどを全て負担した上で、事業運営を行わなければならない。電子マネーは、基本的にプリペイド（ユーザが先に入金、もしくは仮入金する）方式を採用していることから、他の決済方法（例えば、クレジットカードやデビットカードなど）より、手数料を高くすることはできないため、初期投資に対して、採算を上げることが困難であった。

【０００７】

また、それぞれの事業ドメインを独立させ、1つのブランドホルダに対して、複数のアクワイアラおよび複数のイシュアが提携することにより、電子マネー事業が行われる場合、事業運営のための初期投資を、各事業ドメインに分散して負担させることができるため、それぞれの1つの事業体としての初期投資の負担を軽減することができる。しかしながら、複数の事業体の提携による電子マネーシステムにおいては、その事業形態が複雑なものとなり、それぞれの事業ドメインに応じて、事業全体におけるレベニューシェアを行うことが困難である。

【０００８】

そして、１枚のＩＣカードが複数のサービス提供者によって相互運用される場合、あるサービス提供者が提供する固有のサービスに関する情報やアプリケーションは、相互運用する他のサービス提供者から許可なくアクセスできないようにしなければならない。そのようなセキュリティを維持しつつ、相互運用するサービスに関する情報やアプリケーションは、相互運用を実施しているサービス提供者で共有することができるようにしなければならない。

【０００９】

しかしながら、ブランドホルダ、アクワイアラ、およびイシュアをそれぞれ独立させた場合、事業ドメインの分散により、ＩＣカードへの電子マネーの充填や、加盟店において電子マネーを利用するときに必要な認証処理に用いられる暗号鍵の配布および管理が複雑となるため、事業システムの維持・管理のコストアップにつながっていた。

【００１０】

本発明はこのような状況に鑑みてなされたものであり、電子マネー事業において、１つのブランドに対して、多くのイシュアおよび加盟店が参画することができ、イシュアおよび加盟店に対する暗号鍵の配布、およびシステムの運営・管理に必要となるコストを低減することができるようにするものである。

【００１１】

【課題を解決するための手段】

本発明の情報処理装置は、電子マネー情報、および電子マネーサービスに関す

る認証処理に用いられる認証情報が記録される第１の情報処理装置を発行する第２の事業者が管理する第２の情報処理装置と情報を授受する第１の授受手段と、電子マネーを利用したサービスを提供する第３の事業者が管理する第３の情報処理装置と情報を授受する第２の授受手段と、電子マネーサービスに関する認証処理に用いられる認証情報を記録する第１の記録手段と、第２の事業者に関する情報、および第１の事業者と第２の事業者との提携内容に関する情報を記録する第２の記録手段と、第３の事業者に関する情報、および第１の事業者と第３の事業者との提携内容に関する情報を記録する第３の記録手段とを備え、第１の授受手段は、第２の記録手段により記録された第１の事業者と第２の事業者との提携内容に関する情報に基づいて、第１の記録手段により記録された認証情報を出力し、第２の授受手段は、第３の記録手段により記録された第１の事業者と第３の事業者との提携内容に関する情報に基づいて、第１の記録手段により記録された認証情報を出力することを特徴とする。

【００１２】

認証情報は、ＤＥＳを適応した秘密鍵情報を含むものとすることができる。

【００１３】

第２の事業者との課金処理を実行する第１の課金手段と、第３の事業者との課金処理を実行する第２の課金手段とを更に備えさせるようにすることができる。

【００１４】

第１の記録手段により記録された認証情報を用いた認証処理を実行する認証手段を更に備えさせるようにすることができ、認証手段には、第２の授受手段により、第３の事業者より認証処理の実行を要求する信号が入力された場合、第１の記録手段により記録された第３の事業者に対応する認証情報を用いて認証処理を実行させることができる。

【００１５】

第１の情報処理装置に記録された電子マネー情報を書き換える処理を行う第４の情報処理装置と、ネットワークを介して情報を授受する第３の授受手段と、第４の情報処理装置に、第１の情報処理装置に対する電子マネーの充填処理を実行させるための制御信号を生成する生成手段とを更に備えさせることができ、生成

手段には、第２の記録手段により記録された、第１の事業者と第２の事業者との提携内容に関する情報に基づいて、第２の事業者が発行した第１の情報処理装置に対する制御信号を生成させることができ、第３の授受手段には、生成手段により生成された制御信号を、第４の情報処理装置へ出力させることができる。

【００１６】

ネットワークは、インターネットであるものとすることができ、第３の授受手段には、更に、インターネット上に仮想店舗を有する第３の事業者が管理する第５の情報処理装置と情報を授受させることができる。

【００１７】

本発明の情報処理方法は、電子マネー情報、および電子マネーサービスに関する認証処理に用いられる認証情報が記録される第１の情報処理装置を発行する第２の事業者が管理する第２の情報処理装置と情報を授受する第１の授受ステップと、電子マネーを利用したサービスを提供する第３の事業者が管理する第３の情報処理装置と情報を授受する第２の授受ステップと、電子マネーサービスに関する認証処理に用いられる認証情報を記録する第１の記録ステップと、第２の事業者に関する情報、および第１の事業者と第２の事業者との提携内容に関する情報を記録する第２の記録ステップと、第３の事業者に関する情報、および第１の事業者と第３の事業者との提携内容に関する情報を記録する第３の記録ステップとを含み、第１の授受ステップの処理では、第２の記録ステップの処理により記録された第１の事業者と第２の事業者との提携内容に関する情報に基づいて、第１の記録ステップの処理により記録された認証情報を出力し、第２の授受ステップの処理では、第３の記録ステップの処理により記録された第１の事業者と第３の事業者との提携内容に関する情報に基づいて、第１の記録ステップの処理により記録された認証情報を出力することを特徴とする。

【００１８】

本発明の記録媒体に記録されているプログラムは、電子マネー情報、および電子マネーサービスに関する認証処理に用いられる認証情報が記録される第１の情報処理装置を発行する第２の事業者が管理する第２の情報処理装置と情報を授受する第１の授受ステップと、電子マネーを利用したサービスを提供する第３の事

業者が管理する第３の情報処理装置と情報を授受する第２の授受ステップと、電子マネーサービスに関する認証処理に用いられる認証情報を記録する第１の記録ステップと、第２の事業者に関する情報、および第１の事業者と第２の事業者との提携内容に関する情報を記録する第２の記録ステップと、第３の事業者に関する情報、および第１の事業者と第３の事業者との提携内容に関する情報を記録する第３の記録ステップとを含み、第１の授受ステップの処理では、第２の記録ステップの処理により記録された第１の事業者と第２の事業者との提携内容に関する情報に基づいて、第１の記録ステップの処理により記録された認証情報を出力し、第２の授受ステップの処理では、第３の記録ステップの処理により記録された第１の事業者と第３の事業者との提携内容に関する情報に基づいて、第１の記録ステップの処理により記録された認証情報を出力することを特徴とする。

【００１９】

本発明の電子マネーサービス提供システムは、第１の情報処理装置が、第２の事業者が管理する第３の情報処理装置と情報を授受する第１の授受手段と、第３の事業者が管理する第４の情報処理装置と情報を授受する第２の授受手段と、電子マネーサービスに関する認証処理に用いられる認証情報を記録する第１の記録手段と、第２の事業者に関する情報、および第１の事業者と第２の事業者との提携内容に関する情報を記録する第２の記録手段と、第３の事業者に関する情報、および第１の事業者と第３の事業者との提携内容に関する情報を記録する第３の記録手段とを備え、第１の授受手段は、第２の記録手段により記録された第１の事業者と第２の事業者との提携内容に関する情報に基づいて、第１の記録手段により記録された認証情報を出力し、第２の授受手段は、第３の記録手段により記録された第１の事業者と第３の事業者との提携内容に関する情報に基づいて、第１の記録手段により記録された認証情報を出力し、第２の情報処理装置が、第１の授受手段によって、第３の情報処理装置へ出力された認証情報を記録する第４の記録手段と、電子マネー情報を記録する第５の記録手段とを備え、第３の情報処理装置が、第１の情報処理装置と情報を授受する第３の授受手段と、第３の授受手段により入力された認証情報を記録する第６の記録手段と、第２の情報処理装置の発行に関する情報を記録する第７の記録手段と、第６の記録手段により記

録された認証情報に基づいて、第２の情報処理装置との認証処理を実行する第１の認証処理実行手段とを備え、第４の情報処理装置が、第１の情報処理装置と情報を授受する第４の授受手段と、第４の授受手段により入力された認証情報を記録する第８の記録手段と、第８の記録手段により記録された認証情報に基づいて、第２の情報処理装置との認証処理を実行する第２の認証処理実行手段とを備えることを特徴とする。

【００２０】

第３の情報処理装置には、第２の情報処理装置の第５の記録手段により記録された電子マネー情報を書き換える処理を実行する複数の第５の情報処理装置と情報を授受する第５の授受手段を更に備えさせることができ、第１の認証手段には、第５の授受手段により入力された、第２の情報処理装置の第４の記録手段により記録された認証情報に基づいて認証処理を実行させることができる。

【００２１】

第４の情報処理装置には、第２の情報処理装置の第５の記録手段により記録された電子マネー情報を書き換える処理を実行する複数の第５の情報処理装置と情報を授受する第５の授受手段を更に備えさせることができ、第２の認証手段には、第５の授受手段により入力された、第２の情報処理装置の第４の記録手段により記録された認証情報に基づいて認証処理を実行させることができる。

【００２２】

第４の情報処理装置には、第２の情報処理装置と情報を授受する第５の授受手段と、第２の情報処理装置の第５の記録手段により記録された電子マネー情報を書き換えさせるための制御信号を生成する生成手段とを更に備えさせることができ、第２の認証手段には、第５の授受手段により入力された、第２の情報処理装置の第４の記録手段により記録された認証情報に基づいて認証処理を実行させることができる。

【００２３】

第２の情報処理装置には、個人認証カード、入退出鍵、定期券、ポイントカード、会員カード、キャッシュカード、クレジットカード、もしくはローンカードのうち、少なくとも一つの機能を実行するアプリケーションを記録する第９の記

録手段を更に備えさせることができる。

【００２４】

第２の情報処理装置は、非接触型ＩＣカードであるものとすることができる。

【００２５】

第２の情報処理装置は、接触型ＩＣカードであるものとすることができる。

【００２６】

第２の情報処理装置は、携帯電話機であるものとすることができる。

【００２７】

第２の情報処理装置は、ＰＤＡであるものとすることができる。

【００２８】

第２の情報処理装置は、パーソナルコンピュータであるものとすることができる。

【００２９】

第２の情報処理装置は、時計であるものとすることができる。

【００３０】

本発明の情報処理装置、情報処理方法、および記録媒体に記録されているプログラムにおいては、電子マネー情報、および電子マネーサービスに関する認証処理に用いられる認証情報が記録される第１の情報処理装置を発行する第２の事業者が管理する第２の情報処理装置と情報が授受され、電子マネーを利用したサービスを提供する第３の事業者が管理する第３の情報処理装置と情報が授受され、電子マネーサービスに関する認証処理に用いられる認証情報が記録され、第２の事業者に関する情報、および第１の事業者と第２の事業者との提携内容に関する情報が記録され、第３の事業者に関する情報、および第１の事業者と第３の事業者との提携内容に関する情報が記録され、第１の事業者と第２の事業者との提携内容に関する情報に基づいて、認証情報が出力され、第１の事業者と第３の事業者との提携内容に関する情報に基づいて、認証情報が出力される。

【００３１】

本発明の電子マネーサービス提供システムにおいては、第１の情報処理装置で、第２の事業者が管理する第３の情報処理装置と情報が授受され、第３の事業者

が管理する第４の情報処理装置と情報が授受され、電子マネーサービスに関する認証処理に用いられる認証情報が記録され、第２の事業者に関する情報、および第１の事業者と第２の事業者との提携内容に関する情報が記録され、第３の事業者に関する情報、および第１の事業者と第３の事業者との提携内容に関する情報が記録され、第１の事業者と第２の事業者との提携内容に関する情報に基づいて、認証情報が出力され、第１の事業者と第３の事業者との提携内容に関する情報に基づいて、認証情報が出力され、第２の情報処理装置で、認証情報が記録され、電子マネー情報が記録され、第３の情報処理装置で、第１の情報処理装置と情報が授受され、入力された認証情報が記録され、第２の情報処理装置の発行に関する情報が記録され、記録された認証情報に基づいて、第２の情報処理装置との認証処理が実行され、第４の情報処理装置で、第１の情報処理装置と情報が授受され、入力された認証情報が記録され、記録された認証情報に基づいて、第２の情報処理装置との認証処理が実行される。

【００３２】

【発明の実施の形態】

以下、図を参照して、本発明の実施の形態について説明する。

【００３３】

図１は、本発明を適応した電子マネーシステムの構成を示す図である。運営本体としての、アクワイアラ・ブランドホルダ１は、自分自身のブランドの電子マネーに関するサービス（以下、本サービスと称する）の業務を運営するものであり、本サービスと提携しているイシュア２および店舗４に、自分自身が運営・管理するブランドの電子マネーに関する各種処理を実行するために必要となる、全ての「鍵」を管理し、必要に応じて、イシュア２もしくは店舗４に発行する。また、本サービスに参画する店舗４を開拓するのも、アクワイアラ・ブランドホルダ１の業務である。

【００３４】

アクワイアラ・ブランドホルダ１から発行される鍵は、秘密鍵であり、例えば、ＤＥＳ（Data Encryption Standard）などが用いられる。ＤＥＳは、データを64bit単位に区切って暗号化および復号化処理を行う暗号システムである。ＤＥ

Ｓアルゴリズムでは暗号化と復号化は対称であり、受信した暗号文を、同じ鍵を使ってもう一度変換することにより、元の情報を復元することができる。

【００３５】

ＤＥＳでは、簡単なビット位置転置とXOR演算の組み合わせ論理を１６回繰り返している。内部的には、データのフィードバックや条件判断部分がなく、処理が逐次的なので、パイプライン化すれば高速に処理することができる。もともとLSI化することを前提にして決められたアルゴリズムであり、ＤＥＳチップも多く作られている。

【００３６】

イシュア２は、例えば、銀行、クレジットカード会社、鉄道会社、その他の事業者である。アクワイアラ・ブランドホルダ１と提携したイシュア２は、その提携内容に従って、自社が発行する、例えば、ＩＣカードなどに、アクワイアラ・ブランドホルダ１が管理・運営するブランドの電子マネーに関する機能を組み込み、アクワイアラ・ブランドホルダ１が発行する鍵を組み込むことができる。

【００３７】

イシュア２が発行するハードウェアは、アクワイアラ・ブランドホルダ１が管理・運営するブランドの電子マネーに関する各種処理を実行するための機能を有し、鍵を安全に保持することができるものであれば、ＩＣカードのみならず、例えば、携帯電話、ＰＤＡ（Personal Digital (Data) Assistants）、パーソナルコンピュータ、もしくは、時計などの、様々な情報処理機器を用いることが可能である。ここでは、イシュア２が発行するハードウェアはＩＣカードであるものとして説明する。

【００３８】

また、イシュア２により発行されるＩＣカードは、電子マネーの利用以外の機能を有することが可能であり、例えば、社員証などの個人認証機能、建物や部屋などの入退出カード（電子キー）、定期券、ポイントカード、会員カード、キャッシュカード、クレジットカード、ローンカードなどの機能を有する（すなわち、ＩＣカード内部に、それらの機能を実現するアプリケーションを記録させる）ことが可能である。

【００３９】

利用者３、すなわちＩＣカードの保有者は、イシュア２が発行したＩＣカードに、イシュア２より発行された価値（すなわち、電子マネー）を記録させることができる。電子マネーに対応する代金は、現金、クレジットカード、もしくは、銀行口座の預金からの引き落としなどにより支払うことができる。利用者３は、ＩＣカードに記録された電子マネーを用いて、本サービスに加盟している店舗４において、例えば、商品を購入したり、サービスの提供を受けるといった消費活動を行うことが可能である。

【００４０】

店舗４は、アクワイアラ・ブランドホルダ１との提携によって、ＩＣカードと各種情報を授受する場合の認証処理に必要な鍵の発行を受け、提携内容に基づいた各種サービスを利用者３に提供する。

【００４１】

店舗４は、利用者３がＩＣカードを利用して得た商品、もしくはサービスに対する代金を、アクワイアラ・ブランドホルダ１に請求する。アクワイアラ・ブランドホルダ１は、イシュア２に対して、代金の請求を行う。利用者３が保有するＩＣカードに対する電子マネーの発行が、現金の入金と引き換えに行われた場合、イシュア２は、電子マネーの発行に対応する入金を既に得ているが、電子マネーの発行が、クレジットカード、もしくは、銀行口座の預金からの引き落としなどの支払方法によって行われた場合、イシュア２は、例えば、銀行やクレジット会社などの金融機関５に対して、電子マネーの発行に対応する代金の請求を行う。金融機関５は、クレジットカード、もしくは、銀行口座の預金からの引き落としなどの支払方法を利用した利用者３に対する従来の請求方法と同様の請求方法で、電子マネーの発行を受けた利用者３に、電子マネーに対応する料金を請求する。

【００４２】

図２を用いて、アクワイアラ・ブランドホルダ１と、イシュア２、本サービスと提携した店舗４に設置されている各種端末装置、インターネット上に公開されている本サービスと提携したサイバー店舗、および、利用者３が有するパーソナ

ルコンピュータとのネットワーク接続の構成、および、アクワイアラ・ブランドホルダ１の鍵の発行について説明する。

【００４３】

アクワイアラ・ブランドホルダ１は、提携しているイシュア２－１および２－２に対して、その提携内容に従って、所定の鍵を発行する。イシュア２－１は、インターネット１１を介して、利用者３へ、直接的なサービスの提供を行っていない。それに対して、イシュア２－２は、インターネット１１を介して、利用者３へ、直接サービスの提供を行っている。イシュア２－１は、アクワイアラ・ブランドホルダ１が発行した鍵を内部に保持するＩＣカード１２－１を利用者３に対して発行する。また、イシュア２－１は、ＩＣカード１２－１に電子マネーを充填するための入金端末装置１３－１を管理する。同様にして、イシュア２－２も、アクワイアラ・ブランドホルダ１が発行した鍵を内部に保持するＩＣカード１２－２を利用者３に対して発行し、ＩＣカード１２－２に電子マネーを充填するための入金端末装置１３－２を管理する。

【００４４】

ここでは、イシュア２－１およびイシュア２－２の２つのイシュアがアクワイアラ・ブランドホルダ１と提携しているものとして説明しているが、インターネット１１を介した利用者３へのサービスを行っていない複数のイシュア、およびインターネット１１を介した利用者３へのサービスを行っている複数のイシュアが、アクワイアラ・ブランドホルダ１と提携し、それぞれ、提携内容に基づいた鍵の発行を受け、その鍵を内部に保持したＩＣカードを利用者３に発行している。以下、イシュア２－１および２－２を個々に区別する必要がない場合、単にイシュア２と総称し、ＩＣカード１２－１および１２－２を個々に区別する必要がない場合、単にＩＣカード１２と総称し、入金端末装置１３－１および１３－２を個々に区別する必要がない場合、単に入金端末装置１３と総称する。

【００４５】

アクワイアラ・ブランドホルダ１は、利用者３が、本サービスと提携している店舗４において、ＩＣカード１２を利用することができるように（すなわち、ＩＣカード１２と、店舗４に備えられた端末装置との情報の授受が可能となるよう

に）、それぞれ、提携内容に基づいた鍵を発行する。アクワイアラ・ブランドホルダ１が行う、店舗４への鍵の発行方法は、大きく３つに分かれる。

【００４６】

例えば、チェーン店などの複数の店舗４を有する企業が、本サービスと提携した場合、アクワイアラ・ブランドホルダ１は、それらの店舗を統括するＰＯＳ（Point of sale）センタ１７に対して鍵を発行して配布する。ＰＯＳセンタ１７が管理する、それぞれの店舗４に設けられている加盟店端末装置１８（図２においては、加盟店端末装置１８を１つだけ図示しているが、実際には、複数の店舗４に、それぞれ加盟店端末装置１８が設置されている）は、ＰＯＳセンタ１７と、例えば、専用線を用いて接続されており、利用者３が、本サービスの電子マネーを、加盟店端末装置１８において利用するとき、加盟店端末装置１８は、ＰＯＳセンタ１７と接続することにより、ＩＣカード１２との認証処理を実行する。

【００４７】

また、加盟店端末装置１８が高度なタンパ技術（半導体チップなどの内部解析や改ざんを物理的及び論理的に防衛する技術）を用いたものであれば、それぞれの加盟店端末装置１８に、ＰＯＳセンタ１７に配布された鍵を記憶させて、加盟店端末装置１８とＩＣカード１２間で認証処理を実行させるようにしても良い。

【００４８】

なお、図２においては、ＰＯＳセンタ１７をひとつだけ図示して説明しているが、複数のＰＯＳセンタ１７が、その提携内容に基づいて、アクワイアラ・ブランドホルダ１から鍵の発行を受け、自分自身が管理している加盟店端末装置１８とＩＣカード１２との間の認証処理を実行するようにしても良いことはもちろんである。

【００４９】

例えば、コンビニエンスストアや駅などに設置されるＭＭＫ（Multi Media KIOSK（マルチメディアキオスク））２０において、本サービスが提供される場合、アクワイアラ・ブランドホルダ１は、それぞれの店舗４に設置されるＭＭＫ２０を統括するＭＭＫセンタ１９に対して鍵を発行して、配布する。

【００５０】

マルチメディア端末の一種であるＭＭＫ２０は、ＡＴＭ（Automatic Teller Machine）と、公共料金の収納代行やＥＣ（Electronics Commerce（電子商取引））機能などを備える端末が融合した多機能型端末のことである。ＭＭＫ２０（図２においては、ＭＭＫ２０を１つだけ図示しているが、実際には、複数の店舗４に、それぞれＭＭＫ２０が設置されている）は、ＭＭＫセンタ１９と、例えば、専用線を用いて接続されており、利用者３が、本サービスの電子マネーを、ＭＭＫ２０において利用するとき、ＭＭＫ２０は、ＭＭＫセンタ１９と接続することにより、ＩＣカード１２との認証処理を実行するが、加盟店端末装置１８の場合と同様に、ＭＭＫ２０が高度なタンパ技術を用いたものであれば、それぞれのＭＭＫ２０に鍵を記憶させて、ＭＭＫ２０とＩＣカード１２との間で認証処理を実行させるようにしても良い。

【００５１】

なお、ＭＭＫ２０が、ＩＣカード１２に対する電子マネー充填サービスを行う機能を有している場合、ＭＭＫセンタ１９は、対応するイシュア２に接続され、電子マネー充填サービスによって発生する課金処理に関する情報を授受することができるようになされる。

【００５２】

また、図２においては、ＭＭＫセンタ１９をひとつだけ図示して説明しているが、複数のＭＭＫセンタ１９が、その提携内容に基づいて、アクワイアラ・ブランドホルダ１から鍵の発行を受け、自分自身が管理しているＭＭＫ２０とＩＣカード１２との間の認証処理を実行するようにしても良いことはもちろんである。

【００５３】

統括して管理する機構がない店舗４が、単独で、本サービスと提携した場合、アクワイアラ・ブランドホルダ１は、それぞれの店舗４に設置される加盟店端末装置２１に対して鍵を発行し、配布する。加盟店端末装置２１は鍵を記憶し、加盟店端末装置２１とＩＣカード１２との間で認証処理が実行される。

【００５４】

あるいは、アクワイアラ・ブランドホルダ１と加盟店端末装置２１とをオンライン化し、鍵を、加盟店端末装置２１に配布せずに、アクワイアラ・ブランドホ

ルダ１に記録させるようにしてもよい。加盟店端末装置２１は、ＩＣカード１２との各種処理の開始時に、アクワイアラ・ブランドホルダ１に認証情報を送信し、認証処理の実行を要求するようにしても良い。この場合、トランザクション毎の処理に対するコストが発生するが、加盟店端末装置２１に高度なタンパ技術を用いる必要がなくなる。

【００５５】

なお、図２においては、加盟店端末装置２１をひとつだけ図示して説明しているが、複数の加盟店端末装置２１が、その提携内容に基づいて、アクワイアラ・ブランドホルダ１から鍵の発行を受け、ＩＣカード１２との間の認証処理を実行するようにしても良いことはもちろんである。

【００５６】

また、利用者３は、パーソナルコンピュータ１４に接続されたリーダライタ１５を用いて、ＩＣカード１２との情報の授受を行わせることにより、店舗４に赴くことなく、インターネット１１を介して、例えば、イシュア２－２と接続し、電子マネーの充填を行ったり、インターネット１１上に公開されているサイバー店舗１６において、商品を購入することが可能である。サイバー店舗１６は、インターネット１１と接続され、インターネット１１上に、商品やサービスを紹介したり、販売するためのウェブコンテンツを公開し、インターネット１１、パーソナルコンピュータ１４およびリーダライタ１５を介して、ＩＣカード１２との情報の授受を行うことにより、利用者３に各種サービスを提供できるようになされている。

【００５７】

サイバー店舗１６は、アクワイアラ・ブランドホルダ１との提携により鍵の発行は受けるが、発行された鍵の供給を受けない。アクワイアラ・ブランドホルダ１は、サイバー店舗１６に発行した鍵を自分自身に保存し、サイバー店舗１６からの要求に従って、所定のＩＣカード１２との認証処理を実行する。すなわち、本システムにおいては、インターネット１１を介した鍵の供給は行われないようになされている。

【００５８】

なお、図２においては、サイバー店舗１６、パーソナルコンピュータ１４およびリーダライタ１５をそれぞれひとつだけ図示して説明しているが、複数のサイバー店舗１６が、その提携内容に基づいて、アクワイアラ・ブランドホルダ１から鍵の発行を受け、リーダライタ１５、パーソナルコンピュータ１４、およびインターネット１１を介してＩＣカード１２から認証情報の入力を受け、アクワイアラ・ブランドホルダ１に対して認証処理を要求することにより、利用者３に各種サービスを提供することができるようにようにしても良いことはもちろんである。

【００５９】

図２を用いて説明した鍵をはじめとする情報の授受は、セキュリティを重視して、できる限り専用線を用いて通信することが望ましい。しかしながら、いずれかの接続において、インターネット１１などの広域ネットワークを使用せざるを得ない場合、送受信される情報は、例えば、ＳＳＬ（Secure Sockets Layer）などを用いて暗号化される。

【００６０】

また、鍵を含む認証情報や、ＩＣカード１２の電子マネーの残高に関する情報などの特に重要な情報については、例えば、本システム独自の暗号化・復号ルールを制定して、それらに基づいて情報の授受がなされるようにしても良い。なお、これらの情報の通信において、インターネット１１などの広域ネットワークを使用せざるを得ない場合、送受信される情報は、本システム独自のルールに基づいて暗号化され、更にＳＳＬにより暗号化されるようにしてもよい。

【００６１】

なお、アクワイアラ・ブランドホルダ１から供給される鍵は、例えば、磁気ディスク（フロッピーディスクを含む）、光ディスク（CD-ROM (Compact Disk-Read Only Memory)，DVD (Digital Versatile Disk) を含む）、光磁気ディスク（MD(Mini-Disk)を含む）、あるいは、半導体メモリなどのリムーバブルメディアに保存して、イシュア２、ＰＯＳセンタ１７、ＭＭＫセンタ１８、もしくは加盟店端末装置２１に対して配布されるようにしても良い。

【００６２】

このようなシステムを構成することにより、店舗４、多くの店舗４を有する企業（例えばコンビニエンスストアなど）、あるいは、実際の販売店としての店舗４を持たないが、ＭＭＫ２０やインターネット１１上のサイバー店舗１６といった形態で事業を展開する企業などは、本システムにおいて、それぞれの事業に合致したサービスを選択して、利用者３に提供することができ、利用者３も、自分自身が享受したいサービスと提携しているＩＣカード１２を発行するイシュア２を選択して、ＩＣカード１２の発行を受けることができる。

【００６３】

また、本システムは、このような自由度の高いシステムであるのにもかかわらず、電子マネーのブランド管理、および認証処理に用いられる鍵の管理が一元化されているため、システム全体としての管理・運営コストを抑えることができ、更に、セキュアな情報の授受を実現することが可能となる。

【００６４】

図２を用いて説明したように、本サービスに提携しているイシュア２、ＰＯＳセンタ１７、ＭＭＫセンタ１８、および加盟店端末装置２１には、アクワイアラ・ブランドホルダ１から、その提携内容に基づいた鍵が発行され、供給される。入金端末装置１３、加盟店端末装置１８および２１、ＭＭＫ２０には、それぞれ、リーダライタおよびリーダライタを制御するコントローラが含まれ、ＩＣカード１２と、非接触もしくは電気的接触により通信が行われるようになされている。ここでは、ＩＣカード１２とリーダライタは、非接触通信を行うものとし、入金端末装置１３、加盟店端末装置１８および２１、ＭＭＫ２０には、それぞれ、図３に示されるリーダライタ３１およびコントローラ３２が含まれているものとする。

【００６５】

図３に示される非接触カードシステムにおいては、リーダライタ３１とＩＣカード１２との間では、電磁波を利用して非接触でデータの送受信が行われるようになされている。すなわち、リーダライタ３１が、所定のコマンドをＩＣカード１２に送信し、ＩＣカード１２は、そのコマンドを受信し、そのコマンドに対応する処理を行う。そして、ＩＣカード１２は、その処理結果に対応する応答デー

タをリーダライタ３１に送信する。

【００６６】

リーダライタ３１は、所定のインターフェース（例えば、ＲＳ－４８５Ａの規格などに準拠したもの）を介してコントローラ３２に接続されており、コントローラ３２は、リーダライタ３１に対して所定の制御信号を供給することで、所定の処理を行わせる。

【００６７】

図４は、リーダライタ３１の構成を示すブロック図である。なお、図２のリーダライタ１５も、基本的に図４のリーダライタ３１と同様の構成を有するものであるので、その説明は省略する。

【００６８】

ＩＣ４１は、データの処理を行うＤＰＵ（Data Processing Unit）５１、ＩＣカード１２に送信するデータおよびＩＣカード１２から受信したデータの処理を行うＳＰＵ（Signal Processing Unit）５２、コントローラ３２との通信を行うＳＣＣ（Serial Communication Controller）５３、並びに、データの処理に必要な情報を予め記憶しているＲＯＭ（Read Only Memory）６１および処理途中のデータを一時的に記憶するＲＡＭ（Random Access Memory）６２とで構成されるメモリ５４により構成され、ＤＰＵ５１乃至メモリ５４は、バス５５を介して、相互に接続されている。

【００６９】

また、このバス５５には、例えば、認証のために必要なデータ（例えば、アクワイアラ・ブランドホルダ１から供給された鍵など）をはじめとする、所定のデータを記憶するフラッシュメモリ４２、および、ドライブ４７も接続されている。ドライブ４７には、必要に応じて磁気ディスク６５、光ディスク６６、光磁気ディスク６７、および半導体メモリ６８が装着され、データの授受を行う。

【００７０】

アンテナ４６は、所定の電磁波を放射した状態で負荷状態を監視することにより、ＩＣカード１２が装着されたか否かを検出し、装着されたＩＣカード１２に対してデータの送受信を行う。ＩＣカード１２に対するデータの送受信について

の詳細は後述する。

【００７１】

復調回路４４は、アンテナ４６を介して受信した変調波（ＡＳＫ（Amplitude Shift Keying）変調波）を復調し、復調されたデータをＳＰＵ５２に出力する。

【００７２】

ＳＰＵ５２は、復調回路４４を介して、ＩＣカード１２から送信された応答データの入力を受け、そのデータに対して所定の処理（例えば、ＢＰＳＫ（Binary Phase Shift Keying）変調（ワンチェスタコードへのコーディング）など）を施すとともに、ＩＣカード１２に送信するコマンドに対しても、同様に、所定の処理を行った後、変調回路４３に出力する。

【００７３】

ＤＰＵ５１は、ＳＰＵ５２およびバス５５を介して、ＩＣカード１２から受信した応答データや、ＳＣＣ５３およびバス５５を介してコントローラ３２から入力される制御信号の入力を受け、入力された応答データや制御信号に従った処理を実行し、ＩＣカード１２に送信するコマンドを、バス５５を介してＳＰＵ５２に出力したり、コントローラ３２に出力するデータを、バス５５を介してＳＣＣ５３に出力する。

【００７４】

変調回路４３は、発振器（ＯＳＣ）４５より供給される所定の周波数（例えば１３．５６ＭＨｚ）の搬送波を、ＳＰＵ５２より供給されるデータに基づいて、ＡＳＫ変調し、生成された変調波を、アンテナ４６を介して、電磁波としてＩＣカード１２に出力する。なお、このとき、変調回路４３は、変調度を１未満にして、ＡＳＫ変調を行うようになされており、これにより、データがローレベルのときにおいても、変調波の最大振幅がゼロにならないようになされている。

【００７５】

ＳＣＣ５３は、コントローラ３２から入力されたデータを、バス５５を介して、ＤＰＵ５１に供給したり、ＤＰＵ５１から、バス５５を介して入力されたデータを、コントローラ３２に出力する。

【００７６】

図５は、図１のＩＣカード１２の構成を示すブロック図である。

【００７７】

ＩＣカード１２のＩＣ７１は、アンテナ７３を介して、リーダライタ３１（もしくは、リーダライタ１５）により送信された変調波を受信する。コンデンサ７２は、アンテナ７３とともにＬＣ回路を構成し、所定の周波数（キャリア周波数）の電磁波に同調（共振）する。

【００７８】

ＩＣ７１のインターフェース部８１は、ＡＳＫ復調部９１で、アンテナ７３を介して受信した変調波（ＡＳＫ変調波）を検波して復調し、復調後のデータを、ＢＰＳＫ復調部８２およびＰＬＬ（Phase Locked Loop）部８３に出力するとともに、電圧レギュレータ９２で、ＡＳＫ復調部９１が検波した信号を安定化し、各回路に直流電源として供給する。また、インターフェース部８１は、発振回路９３でデータのクロック周波数と同一の周波数の信号を発振し、その信号をＰＬＬ部８３に出力する。

【００７９】

更に、ＩＣカード１２からリーダライタ３１へデータを送信する場合、インターフェース部８１のＡＳＫ変調部９４は、演算部８４からＢＰＳＫ変調部８８を介して供給されるデータに対応して、例えば、所定のスイッチング素子をオン／オフさせ、スイッチング素子がオン状態であるときだけ所定の負荷をアンテナ７３に並列に接続させることにより、ＩＣカード１２の電源としてのアンテナ７３の負荷を変動させる。ＡＳＫ変調部９４は、アンテナ７３の負荷の変動により、アンテナ７３を介して受信している変調波をＡＳＫ変調し（リーダライタ３１は、ＩＣカード１２からデータを受信するとき、すなわち、ＩＣカード１２にデータを送信させるとき、その出力する変調波の最大振幅を一定にしており、この変調波が、アンテナ７３の負荷の変動により、ＡＳＫ変調される）、その変調成分を、アンテナ７３を介してリーダライタ３１に送信する（すなわち、リーダライタ３１のアンテナ４６の端子電圧を変動させる）。

【００８０】

ＰＬＬ部８３は、ＡＳＫ復調部９１より供給されるデータから、そのデータに

同期したクロック信号を生成し、そのクロック信号をＢＰＳＫ復調部８２およびＢＰＳＫ変調部８８に出力する。ＢＰＳＫ復調部８２は、ＡＳＫ復調部９１で復調されたデータが、ＢＰＳＫ変調されている場合、ＰＬＬ部８３より供給されたクロック信号に従って、そのデータの復調（ワンチェスタコードのデコード）を行い、復調したデータを演算部８４に出力する。

【００８１】

演算部８４は、ＢＰＳＫ復調部８２より供給されたデータが暗号化されている場合、そのデータを暗号／復号部９６で復号化した後、そのデータを、シーケンサ９５で処理する。なお、データが暗号化されていない場合、ＢＰＳＫ復調部８２より供給されたデータは、暗号／復号部９６を介さず、シーケンサ９５に、直接供給される。

【００８２】

シーケンサ９５は、入力されるコマンドに従った各種の処理を実行する。すなわち、シーケンサ９５は、例えば、EEPROM（Electrically Erasable and Programmable Read Only Memory）８６に対するデータの書き込みや読み出し、その他データに対する必要な演算処理などを行う。更に、シーケンサ９５は、認証を行うことによるEEPROM８６へのアクセス制御や、EEPROM８６の管理などを実行する。

【００８３】

演算部８４のパリティ演算部９７は、EEPROM８６に記憶されるデータや、EEPROM８６に記憶されているデータから、パリティとして、例えば、リードソロモン符号を算出する。更に、演算部８４は、シーケンサ９５で所定の処理を行った後、その処理に対応する応答データ（リーダライタ３１に送信するデータ）をＢＰＳＫ変調部８８に出力する。ＢＰＳＫ変調部８８は、演算部８４より供給されたデータをＢＰＳＫ変調し、変調後のデータをインターフェース部８１のＡＳＫ変調部９４に出力する。

【００８４】

ＲＯＭ８５は、シーケンサ９５が処理を行うためのプログラム、およびプログラムの実行に必要なデータなどを記憶している。ＲＡＭ８７は、シーケンサ９５

が処理を行うとき、その処理の途中のデータなどを、一時的に記憶する。EEPROM８６は、不揮発性のメモリであり、ＩＣカード１２が、リーダライタ３１との通信を終了し、その電力供給が停止された後も、データを記憶し続ける。

【００８５】

次に、リーダライタ３１とＩＣカード１２との間のデータの送受信処理について説明する。

【００８６】

図４を用いて説明したリーダライタ３１は、アンテナ４６から所定の電磁波を放射した状態で、アンテナ４６の負荷状態を監視し、ＩＣカード１２が接近することによる負荷状態の変化が検出されるまで待機する。なお、リーダライタ３１には、所定の短いパターンのデータでＡＳＫ変調した電磁波を放射して、ＩＣカード１２への呼びかけを、ＩＣカード１２からの応答が一定時間内に得られるまで繰り返す処理（ポーリング）を行わせるようにしてもよい。

【００８７】

リーダライタ３１において、ＩＣカード１２の接近が検出されると、リーダライタ３１のＳＰＵ５２は、所定の周波数（例えば、データのクロック周波数の２倍の周波数）の矩形波を搬送波として、ＩＣカード１２に送信するデータ（例えば、ＩＣカード１２に実行させる処理に対応するコマンドや、ＩＣカード１２に書き込むデータなど）で、ＢＰＳＫ変調を行い、生成した変調波（ＢＰＳＫ変調信号）を変調回路４３に出力する。

【００８８】

なお、ＢＰＳＫ変調時においては、差動変換を利用して、変調波の位相の変化に、データを対応させることができ、この場合、ＢＰＳＫ変調信号が反転しても、元のデータに復調されるので、復調するときに、変調波の極性を配慮する必要が無くなる。

【００８９】

変調回路４３は、入力されたＢＰＳＫ変調信号で、所定の搬送波を１未満（例えば０．１）の変調度（＝データ信号の最大振幅／搬送波の最大振幅）でＡＳＫ変調し、生成された変調波（ＡＳＫ変調波）を、アンテナ４６を介してＩＣカー

ド１２に送信する。

【００９０】

なお、送信を行わないとき、変調回路４３は、ディジタル信号の２つのレベル（ハイレベルとローレベル）のうちの、例えばハイレベルで変調波を生成するようになされている。

【００９１】

図５を用いて説明したＩＣカード１２では、アンテナ７３およびコンデンサ７２で構成されるＬＣ回路において、リーダライタ３１のアンテナ４６が放射した電磁波の一部が電気信号に変換され、その電気信号（変調波）が、ＩＣ７１のインターフェース部８１に出力される。そして、インターフェース部８１のＡＳＫ復調部９１は、その変調波を整流平滑化することで、包絡線検波を行い、これにより生成される信号を電圧レギュレータ９２に供給するとともに、その信号の直流成分を抑制してデータ信号を抽出し、そのデータ信号をＢＰＳＫ復調部８２およびＰＬＬ部８３に出力する。

【００９２】

なお、このとき、アンテナ７３の端子電圧V_0は、例えば次の式（１）で表される。

$$V_0=V_{10}(1+k\times Vs(t))\cos(\omega t)\cdots(1)$$

但し、$V_{10}\cos(\omega t)$は、搬送波を、ｋは変調度を、Ｖｓ（ｔ）はＳＰＵ５２が出力するデータを、それぞれ表す。

【００９３】

また、ＡＳＫ復調部９１による整流後の電圧V_1におけるローレベルの値V_{LR}は、例えば次の式（２）で表される。

$$V_{LR}=V_{10}(1+k\times(-1))-Vf\cdots(2)$$

【００９４】

ここで、Ｖｆは、ＡＳＫ復調部９１において、整流平滑化を行うための整流回路を構成するダイオード（図示せず）における電圧降下を示しており、一般に０．７ボルト程度である。

【００９５】

電圧レギュレータ９２は、ＡＳＫ復調部９１により整流平滑化された信号を受信すると、その信号を安定化し、直流電源として、演算部８４を始めとする各回路に供給する。なお、ここでは、上述したように、変調波の変調度ｋは１未満であるので、整流後の電圧変動（ハイレベルとローレベルの差）が小さい。従って、電圧レギュレータ９２において、直流電源を容易に生成することができる。

【００９６】

ここで、例えば、変調度ｋが５％の変調波を、V_{10}が３ボルト以上になるように受信した場合、整流後のローレベル電圧V_{LR}は、２．１５（＝３×（１－０．０５）－０．７）ボルト以上となり、電圧レギュレータ９２は、電源として充分な電圧を各回路に供給することができる。更に、この場合、整流後の電圧V_1の交流成分（データ成分）の振幅$2\times k\times V_{10}$（Peak-to-Peak値）は、０．３（＝２×０．０５×３）ボルト以上になり、ＡＳＫ復調部９１は、十分高いＳ／Ｎ比でデータの復調を行うことができる。

【００９７】

このように、変調度ｋが１未満のＡＳＫ変調波を利用することにより、エラーレートの低い（すなわち、Ｓ／Ｎ比の高い）状態での通信が実現されるとともに、電源として充分な直流電圧がＩＣカード１２に供給される。

【００９８】

ＢＰＳＫ復調部８２は、ＡＳＫ復調部９１からデータ（ＢＰＳＫ変調信号）を受信すると、そのデータを、ＰＬＬ部８３より供給されるクロック信号に従って復調し、復調したデータを演算部８４に出力する。

【００９９】

演算部８４は、ＢＰＳＫ復調部８２より供給されたデータが暗号化されている場合は、暗号／復号部９６で復号化した後、そのデータをシーケンサ９５に供給して処理する。なお、リーダライタ３１は、この期間、すなわち、ＩＣカード１２にデータを送信後、それに対する返答を受信するまでの間、値が１のデータを送信したまま待機している。従って、この期間においては、ＩＣカード１２は、最大振幅が一定である変調波を受信している。

【０１００】

シーケンサ９５は、処理が終了すると、その処理結果などについての応答データ（リーダライタ３１に送信するデータ）を、ＢＰＳＫ変調部８８に出力する。ＢＰＳＫ変調部８８は、入力されたデータをＢＰＳＫ変調（ワンチェスタコードにコーディング）した後、インターフェース部８１のＡＳＫ変調部９４に出力する。

【０１０１】

そして、ＡＳＫ変調部９４は、アンテナ７３の両端に接続される負荷を、スイッチング素子などを利用し、ＢＰＳＫ変調部８８からのデータに応じて変動させることにより、受信している変調波（ＩＣカード１２によるデータの送信時においては、上述したように、リーダライタ３１が出力する変調波の最大振幅は一定とされている）を、送信するデータに応じてＡＳＫ変調し、これによりリーダライタ３１のアンテナ４６の端子電圧を変動させて、そのデータをリーダライタ３１に送信する。

【０１０２】

一方、リーダライタ３１の変調回路４３は、ＩＣカード１２からのデータの受信時においては、値が１（ハイレベル）のデータの送信を継続している。そして、復調回路４４において、ＩＣカード１２のアンテナ７３と電磁気的に結合しているアンテナ４６の端子電圧の微小な変動（例えば、数十マイクロボルト）から、ＩＣカード１２により送信されたデータが検出される。

【０１０３】

更に、復調回路４４では、検出した信号（ＡＳＫ変調波）が高利得の増幅器（図示せず）で増幅されて復調され、その結果得られるディジタルデータがＳＰＵ５２に出力される。ＳＰＵ５２は、入力されたデータ（ＢＰＳＫ変調信号）を復調し、バス５５を介して、ＤＰＵ５１に出力する。ＤＰＵ５１は、ＳＰＵ５２から入力されたデータを処理し、その処理結果に応じて、通信を終了するか否かを判断する。そして、再度、通信を行うと判断された場合、上述した場合と同様にして、リーダライタ３１とＩＣカード１２との間で通信が行われる。一方、通信を終了すると判断された場合、リーダライタ３１とＩＣカード１２との通信処理が終了される。

【０１０４】

以上のように、リーダライタ３１は、変調度ｋが１未満であるＡＳＫ変調を利用して、ＩＣカード１２にデータを送信し、ＩＣカード１２は、そのデータを受け取り、そのデータに対応する処理を行って、その処理の結果に対応するデータを、リーダライタ３１に返送する。

【０１０５】

次に、図６を用いて、図５のEEPROM８６の論理フォーマットについて説明する。

【０１０６】

EEPROM８６は、ブロックを単位として構成され、例えば、図６においては、１ブロックは、１６バイトで構成されている。

【０１０７】

更に、図６においては、最も上のブロックの論理アドレスを＃０００００ｈ（ｈ１６進数を表す）として、昇順に、論理アドレスが付されている。なお、図では、論理アドレスとして、＃０００００ｈ乃至＃ＦＦＦＦｈが付されており、従って、６５５３６（＝2^{16}）個のブロックが構成されている。

【０１０８】

それぞれのブロックは、ユーザブロックまたはシステムブロックとして使用されるようになされている。EEPROM８６の各ブロックは、論理アドレスの昇順に、ユーザブロックに割り当てられていき、また、論理アドレスの降順に、システムブロックに割り当てられていくようになされている。すなわち、図６において、ユーザブロックは下方向に、システムブロックは上方向に、それぞれ増えていき、空きブロックがなくなった時点で、ユーザブロックおよびシステムブロックをつくることはできなくなる。従って、ユーザブロックとシステムブロックとの境界は固定ではなく、また、ユーザブロックの数、またはシステムブロックの数それぞれには、特に制限がない（但し、図６の場合においては、ユーザブロックとシステムブロックとの合計は、６５５３６個以下に制限される）。

【０１０９】

システムブロックには、製造ＩＤ（Identification）ブロック、発行ＩＤブロ

ック、システム定義ブロック、エリア定義ブロック、サービス定義ブロックの５種類がある。なお、図６の場合においては、エリア定義ブロックまたはサービス定義ブロックとなっているブロックを、エリア／サービス定義ブロックと示している。

【０１１０】

システムブロックのうち、製造ＩＤブロック、発行ＩＤブロック、システム定義ブロックの３つは、基本的に、ＩＣカード１２の発行時には、既に配置されているもので、論理アドレス＃ＦＦＦＦｈ，＃ＦＦＦＥｈ，＃ＦＦＦＤｈにそれぞれ配置される。そして、エリア／サービス定義ブロックは、論理アドレス＃ＦＦＦＣｈより上に、作成順に配置されていく。

【０１１１】

製造ＩＤブロックには、ＩＣカード１２の製造に関する情報が配置される。すなわち、製造ＩＤブロックには、例えば、ユニークな製造ＩＤ、製造年月日、あるいは製造者のコードなどが配置される。

【０１１２】

発行ＩＤブロックには、ＩＣカード１２の発行に関する情報が配置される。すなわち、発行ＩＤブロックには、例えば、ＩＣカード１２が発行された日付、ＩＣカード１２を発行した順番を表すコード、あるいは、カードＩＤなどが配置される。

【０１１３】

システム定義ブロックには、例えば、EEPROM８６が有するシステムブロックまたはユーザブロックの数や、ＩＣカード１２を発行したイシュア２が、アクワイアラ・ブランドホルダ１から配布された鍵などが配置される。この鍵は、上述したように、ＩＣカード１２と、リーダライタ３１およびコントローラ３２との間で、相互認証を行うときに用いられる。

【０１１４】

エリア定義ブロックは、例えば、EEPROM８６の記憶領域（エリア）が、本サービスをはじめとする各種サービスを実現させるための記憶領域に割り当てられることにより作成され、それらが配置された記憶領域を管理するための情報などが

配置される。すなわち、エリア定義ブロックには、例えば、本サービスに関する情報を記録する領域に対応するコード範囲、それぞれの記憶領域の空き容量などが配置される。

【０１１５】

サービス定義ブロックには、後述する、様々なサービスを提供するためのアプリケーションが配置されているサービス領域を管理するための情報（サービス領域の容量や処理を行うために必要な鍵など）などが配置される。

【０１１６】

次に、図７は、コントローラ３２の構成を示すブロック図である。

【０１１７】

制御部１０１は、内部バス１０２を介して、入力部１０３を用いて入力された各種指令に対応する信号に基づいた各種処理を実行する。メモリ１０４は、制御部１０１が使用するプログラム、演算用のパラメータ、もしくは、プログラムの実行において適宜変化するパラメータなどを格納する。制御部１０１およびメモリ１０４は、内部バス１０２により相互に接続されている。

【０１１８】

内部バス１０２は、入力部１０３、表示部１０５、ドライブ１０６、およびネットワークインターフェース１０７とも接続されている。入力部１０３は、例えば、キーボード、マウスあるいはバーコードリーダなどからなり、制御部１０１に各種の指令、あるいはデータなどを入力するとき操作される。表示部１０５は、例えば、ＣＲＴ（Cathode Ray Tube）等からなり、各種情報をテキスト、もしくはイメージなどで表示する。ドライブ１０６には、必要に応じて磁気ディスク１１１、光ディスク１１２、光磁気ディスク１１３、および半導体メモリ１１４が装着され、データの授受を行う。

【０１１９】

ネットワークインターフェース１０７は、例えば、ＲＳ－４８５Ａを介して、リーダライタ３１に接続されたり、所定のインターフェースケーブルなどを用いてＬＡＮ（Local Aria Network）に接続されたり、図示しない電話回線などを介して、例えばインターネット１１などの広域ネットワークに接続される。

【０１２０】

また、図２を用いて説明したように、リーダライタ１５を、パーソナルコンピュータ１４と接続させることにより、利用者３は、店舗に赴くことなく、ＩＣカード１２を用いた本サービスを享受することが可能となる。図８は、パーソナルコンピュータ１４の構成を示すブロック図である。

【０１２１】

ＣＰＵ１２１は、入出力インターフェース１２２および内部バス１２３を介して、例えば、利用者３が入力部１２４を用いて入力した各種指令に対応する信号や、ネットワークインターフェース１２５を介して入力された信号を受け、それらの信号に基づいた各種処理を実行する。ＲＯＭ１２６は、ＣＰＵ１２１が使用するプログラム（例えば、インターネット１１に公開されているウェブコンテンツを閲覧するためのウェブブラウザなど）や、演算用のパラメータのうちの基本的に固定のデータを格納する。ＲＡＭ１２７は、ＣＰＵ１２１の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。ＣＰＵ１２１、ＲＯＭ１２６、およびＲＡＭ１２７は、内部バス１２３により相互に接続されている。

【０１２２】

内部バス１２３は、入出力インターフェース１２２とも接続されている。入力部１２４は、例えば、キーボードやマウスからなり、ＣＰＵ１２１に各種の指令を入力するとき操作される。表示部１２８は、例えば、ＣＲＴ（Cathode Ray Tube）等からなり、各種情報をテキスト、あるいはイメージなどで表示する。ＨＤＤ（Hard Disk Drive）１２９は、ハードディスクを駆動し、ＣＰＵ１２１が使用するプログラムや、それらのプログラムの処理により生成されたデータを記録または再生させる。ドライブ１３０には、必要に応じて磁気ディスク１３１、光ディスク１３２、光磁気ディスク１３３、および半導体メモリ１３４が装着され、データの授受を行う。ネットワークインターフェース１２５は、図示しない電話回線などを介してインターネット１１と接続され、また、所定の接続ケーブルを用いて、リーダライタ１５と接続され、情報の授受を行う。

【０１２３】

また、図２を用いて説明したＰＯＳセンタ１７およびＭＭＫセンタ１９も、図８のパーソナルコンピュータ１４と、基本的に、同様の構成を有するので、その説明は省略する。

【０１２４】

図９は、アクワイアラ・ブランドホルダ１の構成を示すブロック図である。なお、店舗管理サーバ１４１乃至イシュアＧ／Ｗ（ゲートウェイ）サーバ１５１の内部構成は、基本的に、図８を用いて説明したパーソナルコンピュータ１４と同様であるので、その説明は省略する。

【０１２５】

店舗管理サーバ１４１は、本サービスと提携しているイシュア２および店舗４に関する情報を記録する店舗管理ＤＢ（データベース）１４２を管理するサーバであり、店舗管理ＤＢ１４２には、例えば、本サービスと提携しているイシュア２および店舗４の名称、住所、対応するイシュア２もしくは店舗４との清算処理に利用される金融機関の口座番号、本サービスにおける提携内容、および発行された鍵に対応する鍵ＩＤなどが記録されている。

【０１２６】

顧客サーバ１４２は、本サービスを享受している利用者３（すなわち、アクワイアラ・ブランドホルダ１が管理している電子マネーブランドのサービスの利用者）に関する情報を記録する顧客ＤＢ１４４を管理するサーバであり、顧客ＤＢ１４４には、例えば、顧客の氏名、住所、対応する顧客が有する金融機関の口座番号もしくはクレジットカードのカード番号など、顧客が清算処理に利用する金融機関の情報、および、顧客が保有するＩＣカード１２のカードＩＤなどが記録されている。

【０１２７】

セキュリティサーバ１４５は、本サービスにおいて利用される全ての鍵に関する情報、並びに、それぞれの鍵の発行（配布）先となるイシュア２もしくは店舗４などに関する情報を記録する鍵管理ＤＢ１４６を管理するためのサーバであり、必要に応じて、新たに提携されたイシュア２、もしくは、店舗４に対して発行するべき鍵を検索し、イシュアＧ／Ｗサーバ１５１、もしくは、店舗Ｇ／Ｗサー

バ１４９に出力する。

【０１２８】

課金サーバ１４７は、店舗Ｇ／Ｗサーバ１４９、もしくは、ウェブサーバ１５０から入力される、提携している店舗からの課金情報を基に、課金処理を行い、イシュア２に対する請求金額を算出し、イシュアＧ／Ｗサーバ１５１を介して、対応するイシュア２に出力する。課金処理は、例えば、１週間、１ヶ月などの所定の期間毎に行うようにしても良い。更に、課金サーバは、図１４および図１６を用いて後述する、イシュア２－１が発行したＩＣカード１２に対する電子マネーの充填代行サービスに関する処理も実行し、代行による入金に関する情報を入金代行ＤＢ１４８に記録し、例えば、１週間、１ヶ月などの所定の期間毎に、対応するイシュア２－１との清算処理を行う。

【０１２９】

店舗Ｇ／Ｗサーバ１４９は、図２を用いて説明したＰＯＳセンタ１７、ＭＭＫセンタ１９、および加盟店端末装置２１と接続され、ＰＯＳセンタ１７、ＭＭＫセンタ１９、および加盟店端末装置２１との情報の授受を制御し、入力されたデータを、店舗管理サーバ１４１乃至課金サーバ１４７の対応するサーバに出力する（例えば、ＰＯＳセンタ１７から、課金情報が入力された場合、入力されたデータを、課金サーバ１４７に出力する）サーバである。

【０１３０】

ウェブサーバ１５０は、インターネット１１と接続され、サイバー店舗１６もしくはパーソナルコンピュータ１４との情報の授受を制御し、入力されたデータを、店舗管理サーバ１４１乃至課金サーバ１４７の対応するサーバに出力する（例えば、サイバー店舗１６から、ＩＣカード１２の認証情報が入力された場合、入力されたデータを、セキュリティサーバ１４５に出力する）サーバである。

【０１３１】

イシュアＧ／Ｗサーバ１５１は、イシュア２と接続され、イシュア２との情報の授受を制御し、入力されたデータを、店舗管理サーバ１４１乃至課金サーバ１４７の対応するサーバに出力する（例えば、イシュア２から、新たなサービスに対応する鍵の発行要求が入力された場合、入力されたデータを、セキュリティサ

ーバ１４５に出力する）サーバである。

【０１３２】

図１０は、イシュア２－１の構成を示すブロック図である。

【０１３３】

セキュリティサーバ１６１は、アクワイアラ・ブランドホルダ１から発行された鍵を保存する鍵管理ＤＢ１６２を管理し、ＩＣカード１２発行時に、鍵管理ＤＢ１６２から、必要な鍵を検索して出力したり、店舗Ｇ／Ｗサーバ１６６に接続されている入金端末装置１３から入力されたＩＣカード１２の認証情報を基に、対応する鍵を鍵管理ＤＢ１６２から検索して認証処理を行い、認証処理結果を店舗Ｇ／Ｗサーバ１６６に出力する。

【０１３４】

利用者管理サーバ１６３は、発行したＩＣカード１２を利用する利用者３に関する情報を記録する利用者ＤＢ１６４を管理するサーバであり、利用者登録／ＩＣカード発行用の図示しない処理装置などと接続されている。利用者管理サーバ１６３は、利用者登録／ＩＣカード発行用の図示しない処理装置から、例えば、顧客の氏名、住所、対応する顧客が有する金融機関の口座番号もしくはクレジットカードのカード番号、顧客が清算処理に利用する金融機関の情報、および、顧客が保有するＩＣカード１２のカードＩＤなどの入力を受け、利用者ＤＢ１６４に記録し、セキュリティサーバ１６１から出力された鍵を、利用者登録／ＩＣカード発行用の処理装置に出力する。

【０１３５】

アクワイアラ・ブランドホルダＧ／Ｗサーバ１６５は、アクワイアラ・ブランドホルダ１と接続され、情報の授受を制御し、入力されたデータを、セキュリティサーバ１６１乃至課金サーバ１６７の対応するサーバに出力する（例えば、アクワイアラ・ブランドホルダ１から、新たなサービスに対応する鍵が発行され、入力された場合、入力された鍵を、セキュリティサーバ１６１に出力する）。

【０１３６】

店舗Ｇ／Ｗサーバ１６６は、図２を用いて説明した入金端末装置１３、もしくは、ＭＭＫセンタ１９と接続され、入金端末装置１３、もしくは、ＭＭＫセンタ

１９との情報の授受を制御し、入力されたデータを、セキュリティサーバ１６１乃至課金サーバ１６７の対応するサーバに出力する。例えば、入金端末装置１３から、ＩＣカード１２に対する電子マネーの充填処理に関する情報が入力された場合、入力されたデータを、課金サーバ１６７に出力し、入金端末装置１３から、ＩＣカード１２に関する認証情報が入力された場合、入力されたデータをセキュリティサーバ１６１に出力する。

【０１３７】

課金サーバ１６７は、店舗Ｇ／Ｗサーバ１６６から入力される入金端末装置１３、もしくは、ＭＭＫセンタ１９からの課金情報を基に、ＩＣカード１２への電子マネーの充填処理に関する課金処理を行い、課金処理結果を、入金ＤＢ１６８に記録する。

【０１３８】

図１１は、イシュア２－２の構成を示すブロック図である。なお、図１０のイシュア２－１と対応する部分には同一の符号を付してあり、その説明は適宜省略する（以下、同様）。

【０１３９】

ウェブサーバ１７１は、インターネット１１と接続され、情報の授受を制御し、入力されたデータを、セキュリティサーバ１６１乃至課金サーバ１６７の対応するサーバに出力する（例えば、パーソナルコンピュータ１４から、ＩＣカード１２の認証情報が入力された場合、入力されたデータを、セキュリティサーバ１６１に出力する）サーバである。

【０１４０】

また、課金サーバ１６８は、店舗Ｇ／Ｗサーバ１６６のみならず、ウェブサーバ１７１から入力される、パーソナルコンピュータ１４からの電子マネー充填要求に基づいて、ＩＣカード１２への電子マネーの充填処理に関する課金処理を行い、課金処理結果を、入金ＤＢ１６８に記録する。

【０１４１】

次に、図１２乃至図１６を用いて、ＩＣカード１２への電子マネーの充填処理と、電子マネーの充填処理を実行するための鍵の配置の詳細について説明する。

【０１４２】

まず、図１２を用いて、利用者３が、実際の店舗などに赴いて、入金端末装置１３もしくはＭＭＫ２０を利用して、ＩＣカード１２への電子マネーの充填処理を行うことができるようにするための鍵の配置について説明する。

【０１４３】

アクワイアラ・ブランドホルダ１は、例えば、ＩＣカード１２に対して、データの書き込み（すなわち、電子マネーの充填処理）を実行することを認証する鍵Ａ乃至Ｃを有するものとする。例えば、鍵Ａによって、Ａ信販会社のキャッシングサービスによる電子マネーの充填処理ができ、鍵Ｂによって、Ｂ銀行の口座からの引き落としによる電子マネーの充填処理ができ、鍵Ｃによって、クレジットカードＣによる電子マネーの充填処理ができるものとする。

【０１４４】

そして、イシュア２－３と銀行センタ１８１との契約により、銀行センタ１８１が管理する入金端末装置１３において、Ａ信販会社のキャッシングサービスおよびＢ銀行の口座からの引き落としによる電子マネーの充填処理を行うことができるようにするために、鍵Ａおよび鍵Ｂが必要であるものとする。その場合、アクワイアラ・ブランドホルダ１は、イシュア２－３に対して、銀行センタ１８１に、対応する鍵を発行してよいか否かを確認し、イシュア２－３の許可を得て、銀行センタ１８１に鍵Ａおよび鍵Ｂを発行して配布する。

【０１４５】

なお、銀行センタ１８１は、図８を用いて説明したパーソナルコンピュータ１４と、基本的に、同様の構成を有するので、その説明は省略する。

【０１４６】

同様に、イシュア２－４とＭＭＫセンタ１９との契約により、ＭＭＫセンタ１９が管理するＭＭＫ２０において、Ａ信販会社のキャッシングサービスおよびクレジットカードＣによる電子マネーの充填処理を行うことができるようにするために、鍵Ａおよび鍵Ｃが必要であるものとする。その場合、アクワイアラ・ブランドホルダ１は、イシュア２－４に対して、ＭＭＫセンタ１９に、対応する鍵を発行してよいか否かを確認し、イシュア２－４の許可を得て、ＭＭＫセンタ１９

に鍵Ａおよび鍵Ｃを発行して、配布する。

【０１４７】

すなわち、イシュア２－３が発行したＩＣカード１２に、鍵Ａおよび鍵Ｂが記録されている場合、そのＩＣカード１２の利用者３は、ＭＭＫ２０において、Ａ信販会社のキャッシングサービスによる電子マネーの充填処理を行うことは可能であるが、Ｂ銀行の口座からの引き落としによる電子マネーの充填処理を行うことはできない。同様に、イシュア２－４が発行したＩＣカード１２に、鍵Ａおよび鍵Ｃが記録されている場合、そのＩＣカード１２の利用者３は、銀行センタ１８１が管理する入金端末装置１３において、Ａ信販会社のキャッシングサービスによる電子マネーの充填処理を行うことは可能であるが、クレジットカードＣによる電子マネーの充填処理を行うことはできない。

【０１４８】

これらの電子マネー充填処理に伴う、手数料などの清算方法は、従来の清算処理の考え方と同様に、例えば、アクワイアラ・ブランドホルダ１とイシュア２－３、アクワイアラ・ブランドホルダ１とイシュア２－４、イシュア２－３と銀行センタ１８１、および、イシュア２－４とＭＭＫセンタ１９とのそれぞれの提携内容に基づいて、個別に設定可能なようにしても良いし、本サービスの管理者（すなわち、アクワイアラ・ブランドホルダ１の管理者）が、アクワイアラ・ブランドホルダ１の課金サーバ１４７の処理により管理するようにしても良い。

【０１４９】

なお、図１２においては、銀行センタ１８１に１つの入金端末装置１３が接続され、ＭＭＫセンタ１９に１つのＭＭＫ２０が接続されているものとして説明されているが、銀行センタ１８１およびＭＭＫセンタ１９には、複数の入金端末装置１３およびＭＭＫ２０を接続することができる。また、本サービスには、複数の銀行センタ１８１およびＭＭＫセンタ１９が参画可能であることは言うまでもない。

【０１５０】

図１３のフローチャートを参照して、入金端末装置１３（もしくは、ＭＭＫ２０）を用いたＩＣカード１２への電子マネー充填処理について説明する。ここで

は、入金端末装置１３を用いたＩＣカード１２への電子マネー充填処理として説明するが、ＭＭＫ２０を用いたＩＣカード１２への電子マネー充填処理を実行する場合においても、基本的に同様の処理が実行される。

【０１５１】

ステップＳ１において、入金端末装置１３のリーダライタ３１のアンテナ４６は、所定の電磁波を放射した状態で負荷状態を監視することにより、ＩＣカード１２を検出し、ＤＰＵ５１は、ＩＣカード１２を検出したことを示す信号を生成し、バス５５およびＳＣＣ５３を介してコントローラ３２に出力する。

【０１５２】

ステップＳ２において、コントローラ３２の制御部１０１は、ネットワークインターフェース１０７および内部バス１０２を介して、リーダライタ３１から送信されたＩＣカード１２を検出したことを示す信号の入力を受け、利用者３に次の操作を促すためのメッセージなどを含むメニュー画面に対応するデータを、内部バス１０２を介して、表示部１０５に出力して、メニュー画面を表示させる。

【０１５３】

ステップＳ３において、コントローラ３２の制御部１０１は、内部バス１０２を介して、入力部１０３を用いて利用者３が入力したコマンド（例えば、５０００円分の電子マネー充填処理を指令するコマンド）の入力を受け、内部バス１０２およびネットワークインターフェース１０７を介して、リーダライタ３１に出力し、リーダライタ３１は、所定の処理を実行して、入力されたコマンドをＩＣカード１２に送信する。

【０１５４】

ステップＳ４において、ＩＣカード１２のアンテナ７３は、リーダライタ３１より、変調波を受信し、インターフェース部８１、ＢＰＳＫ復調部８２、および演算部８４において所定の処理が実行され、受信されたコマンドに対応する鍵を含む認証情報が、EEPROM８６から読み出される。読み出された認証情報は、演算部８４、ＢＰＳＫ変調部８８、およびインターフェース部８１において所定の処理を施され、アンテナ７３を介して、リーダライタ３１に送出される。

【０１５５】

ステップＳ５において、リーダライタ３１のアンテナ４６は、ＩＣカード１２から送信された認証情報を受信して、復調回路４４に出力する。復調回路４４において復調された認証情報は、ＳＰＵ５２において、ＢＰＳＫ変調などの所定の処理を施され、ＤＰＵ５１に供給される。ＤＰＵ５１は、認証処理を依頼するための信号を生成して、入力された認証情報およびステップＳ３において入力された、利用者３の指令を示すコマンドとともに、バス５５およびＳＣＣ５３を介して、コントローラ３２へ出力する。コントローラ３２の制御部１０１は、ネットワークインターフェース１０７および内部バス１０２を介して、認証処理を依頼するための信号、利用者３の指令を示すコマンド、および認証情報の入力を受け、内部バス１０２およびネットワークインターフェース１０７を介して、対応する銀行センタ１８１に送信する。

【０１５６】

ステップＳ６において、銀行センタ１８１のＣＰＵ１２１（図８は、パーソナルコンピュータ１４のみならず、ＰＯＳセンタ１７、ＭＭＫセンタ１９、もしくは銀行センタ１８１の構成も示す図である）は、ネットワークインターフェース１２５、入出力インターフェース１２２および内部バス１２３を介して入力された認証処理依頼および認証情報に基づいて、アクワイアラ・ブランドホルダ１から供給され、ＲＡＭ１２７もしくはＨＤＤ１２９に保存している鍵を読み出して、認証処理を行う。

【０１５７】

ステップＳ７において、銀行センタ１８１のＣＰＵ１２１は、ステップＳ６において実行された認証処理において、ステップＳ１において検出されたＩＣカード１２は、正しく認証されたか否かを判断する。ステップＳ７において、ＩＣカード１２は正しく認証されなかったと判断された場合、処理は、ステップＳ１６に進む。

【０１５８】

ステップＳ７において、ＩＣカード１２は正しく認証されたと判断された場合、ステップＳ８において、銀行センタ１８１のＣＰＵ１２１は、入力されたコマンドを基に、利用者３が指示した方法（例えば、所定のクレジットカードによる

電子マネー５０００円分の充填など）での価値充填処理、すなわち、ＩＣカード１２に記録されている電子マネーの残額の加算処理は可能か否かを確認する。銀行センタ１８１のＣＰＵ１２１は、例えば、現金による価値の充填が行われる場合、入金端末装置１３に対して、正しい金額の現金が入金されたか否かを確認し、クレジットカードもしくは銀行口座からの引き落としによる価値の充填が行われる場合、イシュア２に対して、電子マネー充填分に対応するクレジットカード利用可能金額の残高、もしくは、銀行口座の残高があるか否かの問い合わせを行う。イシュア２は、例えば、クレジットカード会社や銀行などの所定の金融機関５に対して、対応する利用者３は、価値充填処理に対応する金額のクレジットカード利用、もしくは口座引き落としが可能か否かを問い合わせる。

【０１５９】

ステップＳ９において、銀行センタ１８１のＣＰＵ１２１は、ネットワークインターフェース１２５、入出力インターフェース１２２および内部バス１２３を介して、入金端末装置１３、もしくはイシュア２から入力される、問い合わせに対するレスポンス信号を基に、価値充填処理は可能か否かを判断する。ステップＳ９において、価値充填処理ができないと判断された場合、処理は、ステップＳ１６に進む。

【０１６０】

ステップＳ９において、価値充填処理が可能であると判断された場合、価値充填処理が可能であることを示す信号の入力を受けた入金端末装置１３のコントローラ３２の制御部１０１は、ステップＳ１０において、価値充填処理が可能であることを示す信号を、内部バス１０２およびネットワークインターフェース１０３を介して、リーダライタ３１に送信する。リーダライタ３１のＤＰＵ５１は、ＳＣＣ５３およびバス５５を介して入力された信号を基に、価値充填処理を実行させる（ＩＣカード１２の対象となるファイルに記録されている電子マネーの値を書き換える）ためのコマンドを、バス５５を介してＳＰＵ５２に出力する。ＳＰＵ５２は、入力されたコマンドに対して、例えば、ＢＰＳＫ変調などの所定の処理を行った後、変調回路４３に出力する。変調回路４３は、発振器４５より供給される所定の周波数の搬送波を、ＳＰＵ５２より供給されるデータに基づいて

ＡＳＫ変調し、生成された変調波を、アンテナ４６を介して、電磁波としてＩＣカード１２に出力する。

【０１６１】

ステップＳ１１において、ＩＣカード１２のアンテナ７３は、リーダライタ３１のアンテナ４６より、変調波を受信する。そして、受信された変調波は、インターフェース部８１で検波されてＡＳＫ復調され、ＢＰＳＫ復調部８２でＢＰＳＫ復調され、演算部８４の暗号／復号部９６で復号され、シーケンサ９５によってEEPROM８６に記録されたデータの書き換え、すなわち、価値充填処理が実行され、結果が保存される。

【０１６２】

ステップＳ１２において、入金端末装置１３のコントローラ３２の制御部１０１は、内部バス１０２およびネットワークインターフェース１０７を介して、銀行センタ１８１に処理結果を通知する。

【０１６３】

ステップＳ１３において、銀行センタ１８１のＣＰＵ１２１は、ネットワークインターフェース１２５、入出力インターフェース１２２および内部バス１２３を介して、入金端末装置１３から、価値充填処理結果の入力を受け、内部バス１２３、入出力インターフェース１２２およびネットワークインターフェース１２５を介して、イシュア２に処理結果を通知する。イシュア２は、入力された処理結果を、課金サーバ１６７の処理により、入金ＤＢ１６８に記録し、必要に応じて、アクワイアラ・ブランドホルダ１に、処理結果を通知する。なお、価値充填処理結果の通知は、処理が行われる毎に逐次通知するようにしても良いし、例えば１週間や１ヶ月といった、所定の期間毎に行われるようにしても良い。

【０１６４】

ステップＳ１４において、入金端末装置１３のコントローラ３２の制御部１０１は、価値充填処理結果のログをＩＣカード１２に記録させるための制御信号を生成して、内部バス１０２およびネットワークインターフェース１０７を介して、リーダライタ３１に送信し、リーダライタ３１のＤＰＵ５１は、ＳＣＣ５３およびバス５５を介して入力された信号を基に、ＩＣカード１２に送信するコマン

ドを、バス５５を介してＳＰＵ５２に出力する。ＳＰＵ５２および変調回路４３で所定の処理がなされたコマンドは、アンテナ４６を介して、電磁波としてＩＣカード１２に出力される。

【０１６５】

ステップＳ１５において、ＩＣカード１２のアンテナ７３は、リーダライタ３１より、変調波を受信する。そして、インターフェース部８１、ＢＰＳＫ復調部８２、および演算部８４において所定の処理が実行され、EEPROM８６にログが書き込まれて、保存される。

【０１６６】

ステップＳ７において、ＩＣカード１２が正しく認証されなかったと判断された場合、もしくは、ステップＳ９において、価値充填処理が可能ではないと判断された場合、ステップＳ１６において、銀行センタ１８１のＣＰＵ１２１は、内部バス１２３、入出力インターフェース１２２およびネットワークインターフェース１２５を介して、入金端末装置１３に、エラーメッセージを出力する。

【０１６７】

ステップＳ１７において、入金端末装置１３のコントローラ３２の制御部１０１は、入力されたエラーメッセージを、内部バス１０２を介して表示部１０５に出力して、表示させる。

【０１６８】

次に、図１４を用いて、利用者３が、実際の店舗などに赴くことなく、インターネット１１を介して、ＩＣカード１２への電子マネーの充填処理を行うことができるようにするための鍵の配置、および認証処理について説明する。

【０１６９】

アクワイアラ・ブランドホルダ１は、例えば、ＩＣカード１２に対するデータの書き込み（すなわち、電子マネーの充填処理）の実行を認証する鍵Ｄおよび鍵Ｅを有するものとする。例えば、鍵Ｄによって、Ｄ信販会社のキャッシングサービスによる電子マネーの充填処理ができ、鍵Ｅによって、Ｅ銀行の口座からの引き落としによる電子マネーの充填処理ができるものとする。

【０１７０】

そして、イシュア２－２が発行するＩＣカード１２を保有する利用者３が、パーソナルコンピュータ１４－１乃至１４－ｎを用いて、Ｄ信販会社のキャッシングサービスを利用して、インターネット１１を介して、電子マネーの充填処理を行うことができるようにするために、鍵Ｄが必要であるものとする。その場合、アクワイアラ・ブランドホルダ１は、イシュア２－２に鍵Ｄを発行し、配布する。イシュア２－２は、インターネット１１と接続され、リーダライタ１５、パーソナルコンピュータ１４およびインターネット１１を介して入力される、利用者３が有するＩＣカード１２の認証情報と、アクワイアラ・ブランドホルダ１から供給された鍵Ｄを用いて、認証処理を行い、正しく認証処理が行えた場合、電子マネーの充填処理を行う。

【０１７１】

また、イシュア２－１が発行するＩＣカード１２を保有する利用者３が、パーソナルコンピュータ１４－１乃至１４－ｎを用いて、Ｅ銀行の口座からの引き落としを利用して、インターネット１１を介して、電子マネーの充填処理を行うことができるようにするために、鍵Ｅが必要であるものとする。その場合、アクワイアラ・ブランドホルダ１は、イシュア２－１に鍵Ｅを発行し、配布するが、イシュア２－１は、インターネット１１と接続されていないため、アクワイアラ・ブランドホルダ１に対して、入金代行処理を依頼する。アクワイアラ・ブランドホルダ１は、イシュア２－１に対して発行した鍵Ｅを、入金代行処理用の鍵として、鍵管理ＤＢ１４６に記録する。

【０１７２】

アクワイアラ・ブランドホルダ１は、リーダライタ１５、パーソナルコンピュータ１４およびインターネット１１を介して入力される、利用者３が有するＩＣカード１２の認証情報と、鍵管理ＤＢ１４６に記録された鍵Ｅの情報により、認証処理を行い、正しく認証処理された場合、課金サーバ１４７の処理により、電子マネーの充填処理を行い、その結果を入金代行ＤＢ１４８に記録する。

【０１７３】

この場合においても、電子マネー充填処理に伴う、手数料などの清算方法は、従来の清算処理の考え方と同様に、例えば、アクワイアラ・ブランドホルダ１と

イシュア２－１、アクワイアラ・ブランドホルダ１とイシュア２－２とのそれぞれの提携内容に基づいて、個別に設定可能なようにしても良いし、本サービスの管理者（すなわち、アクワイアラ・ブランドホルダ１の管理者）が、アクワイアラ・ブランドホルダ１の課金サーバ１４７の処理により管理するようにしても良い。

【０１７４】

次に、図１５のフローチャートを参照して、イシュア２－２による、インターネット１１を介したＩＣカード１２への電子マネー充填処理について説明する。

【０１７５】

パーソナルコンピュータ１４のＣＰＵ１２１は、ステップＳ２１において、入出力インターフェース１２２および内部バス１２３を介して入力部１２４から入力される、利用者３の操作を示す信号を基に、ＨＤＤ１２９に保存されているウェブブラウザソフトウェアをＲＡＭ１２７にロードして起動させ、ウェブブラウザを立ち上げ、ステップＳ２２において、インターネット１１を介して、イシュア２－２に接続する。

【０１７６】

ステップＳ２３において、イシュア２－２のウェブサーバ１７１は、インターネット１１を介して、パーソナルコンピュータ１４に、入金希望画面に対応するデータを出力する。

【０１７７】

ステップＳ２４において、パーソナルコンピュータ１４のＣＰＵ１２１は、ネットワークインターフェース１２５、入出力インターフェース１２２、および内部バス１２３を介して入力された入金希望画面に対応するデータを、内部バス１２３および入出力インターフェース１２２を介して、表示部１８２に出力して、入金希望画面を表示させる。入金希望画面には、リーダライタ１５とＩＣカード１２が通信可能な状態となるように、ＩＣカード１２を所定の読み取り位置に設置することを促すためのメッセージ、および、操作の入力を促すメニューなどが表示される。ここでは、ＩＣカード１２への価値充填処理が利用者３によって選択され、入力部１２４を用いて指示されたものとする。

【０１７８】

ステップＳ２５において、リーダライタ１５のアンテナ４６は、所定の電磁波を放射した状態で負荷状態を監視することにより、ＩＣカード１２を検出し、ＤＰＵ５１は、ＩＣカード１２を検出したことを示す信号を生成し、バス５５およびＳＣＣ５３を介してパーソナルコンピュータ１４に出力する。

【０１７９】

ステップＳ２６において、リーダライタ１５のＳＣＣ５３は、パーソナルコンピュータ１４より、利用者３が入力したコマンドの入力を受け、バス５５を介して、ＳＰＵ５２に出力し、ＳＰＵ５２および変調回路４３で所定の処理がなされたコマンドは、アンテナ４６を介して、ＩＣカード１２に送信される。

【０１８０】

ステップＳ２７において、図１３のステップＳ４と同様の処理が実行される。

【０１８１】

ステップＳ２８において、リーダライタ１５のアンテナ４６は、ＩＣカード１２から送信された認証情報を受信して、復調回路４４に出力する。復調回路４４において復調されたデータは、ＳＰＵ５２で、ＢＰＳＫ変調などの所定の処理を施され、ＤＰＵ５１に供給される。ＤＰＵ５１は、認証処理を依頼するための信号を生成して、入力された認証情報とともに、バス５５およびＳＣＣ５３を介して、パーソナルコンピュータ１４に送信する。

【０１８２】

ステップＳ２９において、パーソナルコンピュータ１４のＣＰＵ１２１は、ネットワークインターフェース１２５、入出力インターフェース１２２、および内部バス１２３を介して、認証処理依頼および認証情報の入力を受け、利用者３が実行した操作に対応するコマンド（ここでは、ＩＣカード１２への価値充填処理を指令するためのコマンド）とともに、インターネット１１を介して、イシュア２－２に送信する。

【０１８３】

ステップＳ３０において、イシュア２－２のウェブサーバ１７１は、認証処理依頼および認証情報の入力を受け、セキュリティサーバ１６１に出力する。セキ

ユリティサーバ１６１は、入力された認証処理依頼および認証情報に基づいて、自分自身がアクワイアラ・ブランドホルダ１から供給され、鍵管理ＤＢ１６２に保存している鍵との認証処理を行う。

【０１８４】

ステップＳ３１において、セキュリティサーバ１６１は、ステップＳ３０で実行された認証処理において、ステップＳ２５において検出されたＩＣカード１２は、正しく認証されたか否かを判断する。ステップＳ３１において、ＩＣカード１２は正しく認証されなかったと判断された場合、処理は、ステップＳ４１に進む。

【０１８５】

ステップＳ３１において、ＩＣカード１２は正しく認証されたと判断された場合、ステップＳ３２において、課金サーバ１６７は、入力されたコマンドを基に、利用者３が指示した方法（例えば、所定のクレジットカードによる電子マネー５０００円分の充填）での価値充填処理は可能か否か（例えば、電子マネー充填分に対応するクレジット利用可能金額の残高があるか否か）を、所定の金融機関５（クレジットカード会社、あるいは銀行など）に問い合わせることにより、確認する。

【０１８６】

ステップＳ３２において、課金サーバ１６７は、金融機関５から送信された問い合わせに対するレスポンス信号を基に、価値充填処理は可能か否かを判断する。ステップＳ３２において、価値充填処理ができないと判断された場合、処理は、ステップＳ４１に進む。

【０１８７】

ステップＳ３３において、価値充填処理が可能であると判断された場合、イシュア２－２から、インターネット１１、パーソナルコンピュータ１４を介して、価値充填処理が可能であることを示す信号の入力を受けたリーダライタ１５のＤＰＵ５１は、ステップＳ３４において、入力された信号を基に、ＩＣカード１２に送信する、電子マネー充填処理を実行させるためのコマンドを生成して、バス５５を介してＳＰＵ５２に出力する。そして、ＳＰＵ５２および変調回路４３に

おいて所定の処理が実行されてコマンドに対応する変調波が生成され、アンテナ４６を介して、電磁波としてＩＣカード１２に出力される。

【０１８８】

ステップＳ３５において、ＩＣカード１２のアンテナ７３は、リーダライタ１５のアンテナ４６より、変調波を受信する。そして、インターフェース部８１、ＢＰＳＫ復調部８２、および演算部８４において所定の処理が実行され、コマンドに基づいて、EEPROM８６に記録されたデータの書き換え、すなわち、価値充填処理が実行され、結果が保存される。

【０１８９】

ステップＳ３６において、リーダライタ１５のＤＰＵ５１は、バス５５、ＳＣＣ５３、パーソナルコンピュータ１４、およびインターネット１１を介して、イシュア２－２に処理結果を通知する。

【０１９０】

ステップＳ３７において、イシュア２－２のウェブサーバ１７１は、リーダライタ１５から、価値充填処理結果の入力を受け、課金サーバ１６７に供給する。課金サーバ１６７は、入力された価値充填処理結果を、入金ＤＢ１６８に記録する。

【０１９１】

ステップＳ３８において、アクワイアラ・ブランドホルダＧ／Ｗサーバ１６５は、アクワイアラ・ブランドホルダ１に、価値充填処理の結果を通知する。なお、価値充填処理結果の通知は、処理が行われる毎に逐次通知するようにしても良いし、例えば、１週間や１ヶ月といった、所定の期間毎に行われるようにしても良い。

【０１９２】

ステップＳ３９において、リーダライタ１５のＤＰＵ５１は、ＳＣＣ５３およびバス５５を介して入力された信号を基に、価値充填処理結果のログをＩＣカード１２に記録させるためのコマンドを生成して、バス５５を介してＳＰＵ５２に出力する。ＳＰＵ５２および変調回路４３で所定の処理がなされたコマンドは、アンテナ４６を介して、電磁波としてＩＣカード１２に出力される。

【０１９３】

ステップＳ４０において、図１３のステップＳ１５と同様の処理が実行される。

【０１９４】

ステップＳ３１において、ＩＣカード１２が正しく認証されなかったと判断された場合、もしくは、ステップＳ３３において、価値充填処理が可能ではないと判断された場合、ステップＳ４１において、イシュア２－２のウェブサーバ１７１は、インターネット１１を介して、パーソナルコンピュータ１４に、エラーメッセージを出力する。

【０１９５】

ステップＳ４２において、パーソナルコンピュータ１４のＣＰＵ１２１は、ネットワークインターフェース１２５、入出力インターフェース１２２、および内部バス１２３を介して、エラーメッセージの入力を受け、内部バス１２３、入出力インターフェース１２２を介して、入力されたエラーメッセージを表示部１２８に出力して表示させる。

【０１９６】

次に、図１６のフローチャートを参照して、アクワイアラ・ブランドホルダ１の入金代行による、ＩＣカード１２への電子マネー充填処理について説明する。

【０１９７】

ステップＳ５１において、図１５のステップＳ２１と同様の処理が実行される。

【０１９８】

ステップＳ５２において、パーソナルコンピュータ１４のＣＰＵ１２１は、インターネット１１を介して、アクワイアラ・ブランドホルダ１に接続する。

【０１９９】

ステップＳ５３において、アクワイアラ・ブランドホルダ１のウェブサーバ１５０は、インターネット１１を介して、パーソナルコンピュータ１４に、入金希望画面に対応するデータを出力する。

【０２００】

ステップＳ５４乃至ステップＳ５８において、図１５のステップＳ２４乃至ステップＳ２８と同様の処理が実行される。

【０２０１】

ステップＳ５９において、パーソナルコンピュータ１４のＣＰＵ１２１は、ネットワークインターフェース１２５、入出力インターフェース１２２、および内部バス１２３を介して、認証処理依頼および認証情報の入力を受け、利用者３が実行した操作に対応するコマンド（ここでは、ＩＣカード１２への価値充填処理を指令するコマンド）とともに、インターネット１１を介して、アクワイアラ・ブランドホルダ１に送信する。

【０２０２】

ステップＳ６０において、アクワイアラ・ブランドホルダ１のウェブサーバ１５０は、認証処理依頼および認証情報の入力を受け、セキュリティサーバ１４５に出力する。セキュリティサーバ１４５は、入力された認証処理依頼および認証情報に基づいて、鍵管理ＤＢ１４６に保存している鍵を読み出して、認証処理を行う。

【０２０３】

ステップＳ６１において、セキュリティサーバ１４５は、ステップＳ６０の認証処理において、ステップＳ５５において検出されたＩＣカード１２は、正しく認証されたか否かを判断する。ステップＳ６１において、ＩＣカード１２は正しく認証されなかったと判断された場合、処理は、ステップＳ７１に進む。

【０２０４】

ステップＳ６１において、ＩＣカード１２は正しく認証されたと判断された場合、ステップＳ６２において、課金サーバ１４５は、入力されたコマンドを基に、利用者３が指示した方法（例えば、所定のクレジットカードによる電子マネー５０００円分の充填）での価値充填処理は可能か否か（例えば、電子マネー充填分に対応するクレジット利用可能金額の残高があるか否か）を、対応するイシュア２－１に問い合わせることにより、確認する。

【０２０５】

ステップＳ６３において、課金サーバ１４７は、イシュア２－１から送信され

た問い合わせに対するレスポンス信号を基に、価値充填処理は可能か否かを判断する。ステップＳ６３において、価値充填処理ができないと判断された場合、処理は、ステップＳ７１に進む。

【０２０６】

ステップＳ６３において、価値充填処理が可能であると判断された場合、アクワイアラ・ブランドホルダ１から、ＳＣＣ５３およびバス５５を介して、価値充填処理が可能であることを示す信号の入力を受けたリーダライタ１５のＤＰＵ５１は、ステップＳ６４において、図１５のステップＳ３４と同様の処理を実行する。

【０２０７】

ステップＳ６５において、図１５のステップＳ３５と同様の処理が実行される。

【０２０８】

ステップＳ６６において、リーダライタ１５のＤＰＵ５１は、バス５５、ＳＣＣ５３、パーソナルコンピュータ１４、およびインターネット１１を介して、アクワイアラ・ブランドホルダ１に処理結果を通知する。

【０２０９】

ステップＳ６７において、アクワイアラ・ブランドホルダ１のウェブサーバ１５０は、リーダライタ１５から、価値充填処理結果の入力を受け、課金サーバ１４７に供給する。課金サーバ１４７は、入力された価値充填処理結果を、入金代行ＤＢ１４８に記録する。

【０２１０】

ステップＳ６８において、イシュアＧ／Ｗサーバ１５１は、イシュア２－１に、価値充填処理の結果を通知する。なお、価値充填処理結果の通知は、処理が行われる毎に逐次通知するようにしても良いし、例えば１週間や１ヶ月といった、所定の期間毎に行われるようにしても良い。

【０２１１】

ステップＳ６９およびステップＳ７０において、図１５のステップＳ３９およびステップＳ４０と同様の処理が実行される。

【０２１２】

ステップＳ６１において、正しく認証されなかったと判断された場合、もしくは、ステップＳ６３において、価値充填処理が可能ではないと判断された場合、ステップＳ７１において、アクワイアラ・ブランドホルダ１のウェブサーバ１５０は、インターネット１１を介して、パーソナルコンピュータ１４に、エラーメッセージを出力する。

【０２１３】

ステップＳ７２において、図１５のステップＳ４２と同様の処理が実行される。

【０２１４】

次に、図１７乃至図２１を参照して、利用者３が、ＩＣカード１２に充填された電子マネーを用いて商品を購入したり、各種サービスを受けるための処理と、それらの処理を実行するための鍵の配置の詳細について説明する。

【０２１５】

まず、図１７を用いて、利用者３が、実際の店舗などに赴いて、加盟店舗端末装置１８を利用して、ＩＣカード１２へ充填された電子マネーを用いて、商品、もしくはサービスの購入を行うことができるようにするための鍵の配置について説明する。

【０２１６】

図２を用いて上述したように、統括して管理する機構がない店舗４が、単独で、本サービスと提携した場合、アクワイアラ・ブランドホルダ１は、それぞれの店舗４に設置される加盟店端末装置１８に対して、提携内容に基づいて、対応する鍵を発行して配布する。すなわち、図１７の加盟店端末装置１８－１－１乃至１８－１－ｎは、それぞれの店舗４において提供することができるサービスに対応する鍵を、リーダライタ３１－３－１乃至３１－３－ｎにそれぞれ記憶しているので、加盟店端末装置１８とＩＣカード１２との間で認証処理を実行することができる。

【０２１７】

店舗４は、それぞれの事業に合致したサービスを選択して、本サービスとの提

携を結び、アクワイアラ・ブランドホルダ１より対応する鍵の供給を受けることにより、選択したサービスを利用者３に提供することができる。すなわち、鍵Ｆもしくは鍵Ｊが記憶されたＩＣカード１２を保有する利用者３は、加盟店端末装置１８－１－１を設置している店舗において、鍵Ｆもしくは鍵Ｊにより供給可能なサービスを受けることができ、鍵Ｇが記憶されたＩＣカード１２を保有する利用者３は、加盟店端末装置１８－１－２を設置している店舗において、鍵Ｇにより供給可能なサービスを受けることができ、鍵Ｇ、鍵Ｈもしくは鍵Ｊが記憶されたＩＣカード１２を保有する利用者３は、加盟店端末装置１８－１－ｎを設置している店舗において、鍵Ｇ、鍵Ｈもしくは鍵Ｊにより供給可能なサービスを受けることができる。

【０２１８】

例えば、チェーン店などの複数の店舗４を有する企業が本サービスと提供した場合、アクワイアラ・ブランドホルダ１は、複数の店舗４を統括するＰＯＳセンタ１７に対して鍵を発行して、配布する。加盟店端末装置１８－２－１乃至１８－２－ｍは、基本的には、鍵の供給を受けずに、ＰＯＳセンタ１７と接続することにより、ＩＣカード１２との認証処理を実行する（加盟店端末装置１８－２－１乃至１８－２－ｍが高度なタンパ技術を用いたものであれば、加盟店端末装置１８－２－１乃至１８－２－ｍそれぞれに鍵を記憶させて、加盟店端末装置１８－２－１乃至１８－２－ｍとＩＣカード１２間で認証処理を実行させるようにしても良い）。

【０２１９】

すなわち、加盟店端末装置１８－２－１乃至１８－２－ｍにおいて、鍵Ｆもしくは鍵Ｈが記憶されたＩＣカード１２を保有する利用者３は、ＰＯＳセンタ１７に保存されている鍵Ｆもしくは鍵Ｈにより供給可能なサービスを受けることができるが、リーダライタ３１－４－１乃至３１－４－ｍには、鍵Ｆおよび鍵Ｈは保存されていない。

【０２２０】

以下、加盟店舗端末装置１８－１－１乃至１８－１－ｎを個々に区別する必要がない場合、単に加盟店舗端末装置１８－１と総称し、加盟店端末装置１８－２

－１乃至１８－２－ｍを個々に区別する必要がない場合、単に加盟店舗端末装置１８－２と総称する。

【０２２１】

図１８のフローチャートを参照して、ＩＣカード１２を保有する利用者３が、加盟店舗端末装置１８－１を利用して、商品もしくはサービスを購入する場合の処理について説明する。

【０２２２】

ステップＳ８１において、加盟店舗端末装置１８－１のリーダライタ３１のアンテナ４６は、所定の電磁波を放射した状態で負荷状態を監視することにより、ＩＣカード１２を検出し、ＤＰＵ５１は、ＩＣカード１２を検出したことを示す信号を生成し、バス５５およびＳＣＣ５３を介してコントローラ３２に出力する。

【０２２３】

ステップＳ８２において、コントローラ３２の制御部１０１は、ネットワークインターフェース１０７および内部バス１０２を介して、リーダライタ３１から送信された信号の入力を受け、利用者３に次の操作を促すためのメッセージなどを含むメニュー画面に対応するデータを、内部バス１０２を介して、表示部１０５に出力して、メニュー画面を表示させる。

【０２２４】

ステップＳ８３において、コントローラ３２の制御部１０１は、内部バス１０２を介して、入力部１０３からコマンド（例えば、電子マネー２０００円分の利用を示すコマンド）の入力を受け、内部バス１０２およびネットワークインターフェース１０７を介して、リーダライタ３１に出力し、リーダライタ３１は、所定の処理を実行して、入力されたコマンドをＩＣカード１２に送信する。

【０２２５】

ステップＳ８４において、図１３のステップＳ４と同様の処理が実行される。

【０２２６】

ステップＳ８５において、リーダライタ３１のアンテナ４６は、ＩＣカード１２から送信された認証情報を受信して、復調回路４４に出力する。復調回路４４

において復調されたデータは、ＳＰＵ５２で、ＢＰＳＫ変調などの所定の処理が施され、ＤＰＵ５１に供給される。ＤＰＵ５１は、入力された認証情報を基に、バス５５を介して、フラッシュメモリ４２から鍵を読み出し、認証処理を実行する。

【０２２７】

ステップＳ８６において、リーダライタ３１のＤＰＵ５１は、ステップＳ８１において検出されたＩＣカード１２は、正しく認証されたか否かを判断する。ステップＳ８６において、ＩＣカード１２は正しく認証されなかったと判断された場合、処理は、ステップＳ９４に進む。

【０２２８】

ステップＳ８６において、ＩＣカード１２は正しく認証されたと判断された場合、ステップＳ８７において、リーダライタ３１のＤＰＵ５１は、入力されたコマンドを基に、利用者３が指示したＩＣカード利用処理は可能か否かを、ＩＣカード１２から必要な情報を読み出すことなどにより確認する。例えば、２０００円分の商品の購入を指示するコマンドが入力された場合、リーダライタ３１のＤＰＵ５１は、ＩＣカード１２に、商品の代金に対応する電子マネーが残っているか否かを確認するためのコマンドを生成し、所定の処理を実行して、生成したコマンドをＩＣカード１２に送信する。

【０２２９】

ステップＳ８８において、リーダライタ３１のＤＰＵ５１は、アンテナ４６を介して、ＩＣカード１２から入力される問い合わせに対するレスポンス信号などを基に、コマンド処理は可能か否かを判断する。ステップＳ８８において、コマンド処理ができないと判断された場合、処理は、ステップＳ９４に進む。

【０２３０】

ステップＳ８８において、コマンド処理が可能であると判断された場合、ステップＳ８９において、リーダライタ３１のＤＰＵ５１は、ＩＣカード１２に対して価値充填処理を実行させる（ＩＣカード１２の対象となるファイルに記録されている電子マネーの値から、所定の値を減算させる）ためのコマンドを生成して、バス５５を介してＳＰＵ５２に出力する。そして、ＳＰＵ５２および変調回路

４３において所定の処理が施されて、コマンドに対応する変調波が生成され、アンテナ４６を介して、電磁波としてＩＣカード１２に出力される。

【０２３１】

ステップＳ９０において、ＩＣカード１２のアンテナ７３は、リーダライタ３１のアンテナ４６より、変調波を受信する。そして、インターフェース部８１、ＢＰＳＫ復調部８２、および演算部８４において所定の処理が実行され、EEPROM８６に記録された電子マネーの減算に対応するコマンド処理が実行され、結果が保存される。

【０２３２】

ステップＳ９１において、コントローラ３２の制御部１０１は、コマンド処理結果を、内部バス１０２およびネットワークインターフェース１０７を介して、アクワイアラ・ブランドホルダ１に通知する。なお、コマンド処理結果の通知は、処理が行われる毎に逐次通知するようにしても良いし、例えば１週間や１ヶ月といった、所定の期間毎に行われるようにしても良い。

【０２３３】

ステップＳ９２において、コントローラ３２の制御部１０１は、コマンド処理結果のログをＩＣカード１２に記録させるための制御信号を生成して、内部バス１０２およびネットワークインターフェース１０７を介して、リーダライタ３１に送信し、リーダライタ３１のＤＰＵ５１は、ＳＣＣ５３およびバス５５を介して入力された信号を基に、ＩＣカード１２に送信するコマンドを、バス５５を介してＳＰＵ５２に出力する。ＳＰＵ５２および変調回路４３で所定の処理が施されて、コマンドに対応する変調波が生成され、アンテナ４６を介して、電磁波としてＩＣカード１２に出力される。

【０２３４】

ステップＳ９３において、ＩＣカード１２のアンテナ７３は、リーダライタ３１より、変調波を受信する。そして、インターフェース部８１、ＢＰＳＫ復調部８２、および演算部８４において所定の処理が実行され、EEPROM８６にコマンド処理のログが書き込まれ、保存される。

【０２３５】

ステップＳ８６において、ＩＣカード１２が正しく認証されなかったと判断された場合、もしくは、ステップＳ８８において、コマンド処理が可能ではないと判断された場合、ステップＳ９４において、コントローラ３２の制御部１０１は、内部バス１０２を介して、表示部１０５にエラーメッセージを出力して、表示させる。

【０２３６】

次に、図１９のフローチャートを参照して、ＩＣカード１２を保有する利用者３が、加盟店舗端末装置１８－２を利用して、商品、もしくはサービスを購入する場合の処理について説明する。

【０２３７】

ステップＳ１０１乃至ステップＳ１０４において、図１８のステップＳ８１乃至ステップＳ８４と同様の処理が実行される。

【０２３８】

ステップＳ１０５において、リーダライタ３１のアンテナ４６は、ＩＣカード１２から送信された認証情報を受信して、復調回路４４に出力する。復調回路４４において復調されたデータは、ＳＰＵ５２で、ＢＰＳＫ変調などの所定の処理が施され、ＤＰＵ５１に供給される。ＤＰＵ５１は、認証処理を依頼するための信号を生成して、バス５５およびＳＣＣ５３を介して、入力された認証情報とともに、コントローラ３２へ出力する。コントローラ３２の制御部１０１は、ネットワークインターフェース１０７および内部バス１０２を介して、認証処理を依頼するための信号、および認証情報の入力を受け、内部バス１０２およびネットワークインターフェース１０７を介して、利用者３の指令を示すコマンドとともに、対応するＰＯＳセンタ１７に送信する。

【０２３９】

ステップＳ１０６において、ＰＯＳセンタ１７のＣＰＵ１２１は、ネットワークインターフェース１２５、入出力インターフェース１２２および内部バス１２３を介して入力された認証処理依頼および認証情報に基づいて、アクワイアラ・ブランドホルダ１から供給され、ＲＡＭ１２７もしくはＨＤＤ１２９に保存している鍵を読み出して認証処理を行う。

【０２４０】

ステップＳ１０７において、ＰＯＳセンタ１７のＣＰＵ１２１は、ステップＳ１０６で実行された認証処理において、ステップＳ１０１において検出されたＩＣカード１２は、正しく認証されたか否かを判断する。ステップＳ１０７において、ＩＣカード１２は正しく認証されなかったと判断された場合、処理は、ステップＳ１１７に進む。

【０２４１】

ステップＳ１０７において、ＩＣカード１２は正しく認証されたと判断された場合、ステップＳ１０８において、ＰＯＳセンタ１７のＣＰＵ１２１は、内部バス１２３、入出力インターフェース１２２、およびネットワークインターフェース１２５を介して、正しく認証されたことを、加盟店端末装置１８－２に通知する。

【０２４２】

ステップＳ１０９乃至ステップＳ１１２において、図１８のステップＳ８７乃至ステップＳ９０と、同様の処理が実行される。

【０２４３】

ステップＳ１１３において、コントローラ３２の制御部１０１は、ネットワークインターフェース１０７および内部バス１０２を介して、ＰＯＳセンタ１７に処理結果を通知する。

【０２４４】

ステップＳ１１４において、ＰＯＳセンタ１７のＣＰＵ１２１は、内部バス１２３、入出力インターフェース１２２、およびネットワークインターフェース１２５を介して、コマンド処理結果を、アクワイアラ・ブランドホルダ１に通知する。なお、コマンド処理結果の通知は、処理が行われる毎に逐次通知するようにしても良いし、例えば１週間や１ヶ月といった、所定の期間毎に行われるようにしても良い。

【０２４５】

ステップＳ１１５およびステップＳ１１６において、図１８のステップＳ９２およびステップＳ９３と同様の処理が実行される。

【０２４６】

ステップＳ１０７において、正しく認証されなかったと判断された場合、もしくは、ステップＳ１１０において、コマンド処理が可能ではないと判断された場合、ステップＳ１１７において、ＰＯＳセンタ１７のＣＰＵ１２１は、内部バス１２３、入出力インターフェース１２２、およびネットワークインターフェース１２５を介して、加盟店端末装置１８－２に、エラーメッセージを出力する。

【０２４７】

ステップＳ１０８において、図１８のステップＳ９４と同様の処理が実行される。

【０２４８】

なお、図１７および図１９においては、ＩＣカード１２を保有する利用者３が、加盟店端末装置１８－２を利用する場合の処理について説明したが、ＭＭＫセンタ１９に統括管理されているＭＭＫ２０を利用する場合においても、ＰＯＳセンタ１７に統括管理されている加盟店端末装置１８－２における処理と、基本的に同様の処理が実行される。

【０２４９】

次に、図２０を用いて、利用者３が、実際の店舗などに赴くことなく、ＩＣカード１２に充填された電子マネーを用いて、インターネット１１に公開されているサイバー店舗１６において商品を購入したり、各種サービスを受けるための処理と、それらの処理を実行するための鍵の配置の詳細について説明する。

【０２５０】

インターネット１１と接続している複数のサイバー店舗１６－１乃至１６－ｍは、アクワイアラ・ブランドホルダ１との提携内容に基づいて、インターネット１１に接続することが可能なパーソナルコンピュータ１４－１乃至１４－ｎ、および、パーソナルコンピュータ１４－１乃至１４－ｎに接続されたリーダライタ１５－１乃至１５－ｎを利用する、ＩＣカード１２を保有する利用者３に対して、各種サービスを提供することが可能なようになされている。

【０２５１】

サイバー店舗１６－１乃至１６－ｍは、例えば、インターネット１１を介して

、利用者３が保有するパーソナルコンピュータ１４に、購入希望画面などを出力したり、パーソナルコンピュータ１４から、ＩＣカード１２の認証情報や、利用者３が購入を希望する商品についての情報の入力を受けるためのウェブサーバ１９３－１乃至１９３－ｍ、商品の在庫や売上に関する情報を記録するための在庫／売上管理ＤＢ１９２－１乃至１９２－ｍを管理し、サービス提供に関する処理を実行する売上管理サーバ１９１－１乃至１９１－ｍを備えている。

【０２５２】

以下、売上管理サーバ１９１－１乃至１９１－ｍを個々に区別する必要がない場合、単に、売上管理サーバ１９１と総称し、在庫／売上管理ＤＢ１９２－１乃至１９２－ｍを個々に区別する必要がない場合、単に、在庫／売上管理ＤＢ１９２と総称し、ウェブサーバ１９３－１乃至１９３－ｍを個々に区別する必要がない場合、単に、ウェブサーバ１９３と総称する。なお、売上管理サーバ１９１およびウェブサーバ１９３の構成は、図８を用いて説明したパーソナルコンピュータ１４と基本的に同様であるので、その説明は省略する。

【０２５３】

アクワイアラ･ブランドホルダ１は、サイバー店舗１６－１乃至１６－ｍそれぞれとの提携内容に基づいて、鍵Ｋ、鍵Ｌ、もしくは鍵Ｍを発行した場合においても、発行した鍵をサイバー店舗１６－１乃至１６－ｍに配布しない。アクワイアラ･ブランドホルダ１のセキュリティサーバ１４５は、鍵管理ＤＢ１４６に、サイバー店舗１６－１乃至１６－ｍそれぞれに、いずれの鍵を発行したかを登録しているので、サイバー店舗１６－１乃至１６－ｍのいずれかから、認証処理を依頼された場合、鍵管理ＤＢ１４６を参照して、認証処理を実行し、認証処理結果を、対応するサイバー店舗１６－１乃至１６－ｍのいずれかに、インターネット１１を介して出力する。

【０２５４】

すなわち、サイバー店舗１６－１乃至１６－ｍは、いずれの鍵も記録しない。サイバー店舗１６－１乃至１６－ｍは、インターネット１１を介して、パーソナルコンピュータ１４から、リーダライタ１５で読み込まれたＩＣカード１２の認証情報の入力を受けた場合、その認証情報を、インターネット１１を介して、ア

クワイアラ･ブランドホルダ１に出力し、認証処理を依頼し、インターネット１１を介して、アクワイアラ･ブランドホルダ１から、認証処理結果の入力を受ける。

【０２５５】

図２１のフローチャートを参照して、ＩＣカード１２を保有する利用者３が、パーソナルコンピュータ１４を用いて、インターネット１１を介して、サイバー店舗１６にアクセスし、商品、もしくはサービスを購入する場合の処理について説明する。

【０２５６】

ステップＳ１２１において、図１５のステップＳ２１と同様の処理が実行される。

【０２５７】

ステップＳ１２２において、パーソナルコンピュータ１４のＣＰＵ１２１は、内部バス１２３、入出力インターフェース１２２、ネットワークインターフェース１２５、およびインターネット１１を介して、サイバー店舗１６に接続する。

【０２５８】

ステップＳ１２３において、サイバー店舗１６のウェブサーバ１９３は、インターネット１１を介して、パーソナルコンピュータ１４に、購入希望画面に対応するデータを出力する。

【０２５９】

ステップＳ１２４において、パーソナルコンピュータ１４のＣＰＵ１２１は、ネットワークインターフェース１２５、入出力インターフェース１２２、および内部バス１２３を介して入力された、購入希望画面に対応するデータを、内部バス１２３および入出力インターフェース１２２を介して、表示部１２８に出力して、入力希望画面を表示させる。入力希望画面には、リーダライタ１５とＩＣカード１２が通信可能な状態となるように、ＩＣカード１２を所定の読み取り位置に設置することを促すためのメッセージ、および、操作の入力を促すメニューなどが表示される。ここでは、ＩＣカード１２を用いた商品の購入処理が利用者３によって選択され、入力部１２４を用いて指示されたものとする。

【０２６０】

ステップＳ１２５乃至ステップＳ１２８において、図１５のステップＳ２５乃至ステップＳ２８と同様の処理が実行される。

【０２６１】

ステップＳ１２９において、パーソナルコンピュータ１４のＣＰＵ１２１は、ネットワークインターフェース１２５、入出力インターフェース１２２、および内部バス１２３を介して、認証情報の入力を受け、利用者３が実行した操作に対応するコマンド（ここでは、ＩＣカード１２を用いた商品購入処理を実行するためのコマンド）とともに、サイバー店舗１６に送信する。

【０２６２】

ステップＳ１３０において、サイバー店舗１６のウェブサーバ１９３は、認証情報の入力を受け、アクワイアラ･ブランドホルダ１に対して認証処理を依頼する信号を生成し、入力された認証情報とともに、アクワイアラ･ブランドホルダ１に出力する。アクワイアラ･ブランドホルダ１のウェブサーバ１５０は、入力された情報を、セキュリティサーバ１４５に出力する。セキュリティサーバ１４５は、入力された認証処理依頼および認証情報に基づいて、鍵管理ＤＢ１４６に保存している、対応するサイバー店舗１６に発行した鍵との認証処理を行い、認証処理結果を、インターネット１１を介して、サイバー店舗１６に出力する。

【０２６３】

サイバー店舗１６の売上管理サーバ１９１は、ステップＳ１３１において、アクワイアラ･ブランドホルダ１から、インターネット１１およびウェブサーバ１９３を介して、認証結果の入力を受け、ステップＳ１３２において、ステップＳ１２５において検出されたＩＣカード１２は、正しく認証されたか否かを判断する。ステップＳ１３２において、ＩＣカード１２は正しく認証されなかったと判断された場合、処理は、ステップＳ１４４に進む。

【０２６４】

ステップＳ１３３において、サイバー店舗１６の売上管理サーバ１９１は、正しく認証されたことを、ウェブサーバ１９３、およびインターネット１１を介して、パーソナルコンピュータ１４に通知する。

【０２６５】

ステップＳ１３４において、パーソナルコンピュータ１４のＣＰＵ１２１は、入力された認証結果を、内部バス１２３、入出力インターフェース１２２、および、ネットワークインターフェース１２５を介して、リーダライタ１５に出力する。

【０２６６】

ステップＳ１３５において、リーダライタのＤＰＵ５１は、入力された認証結果を基に、利用者３が指示したＩＣカード利用処理（例えば、２０００円分の商品の購入）は可能か否か（ＩＣカード１２に、商品の代金に対応する電子マネーが残っているか否か）を、ＩＣカード１２から必要な情報を読み出し、パーソナルコンピュータ１４、インターネット１１を介して、アクワイアラ・ブランドホルダ１に、売上承認要求を送信し、そのレスポンスを受けることなどにより確認する。

【０２６７】

ステップＳ１３６において、リーダライタ１５のＤＰＵ５１は、アンテナ４６を介して、ＩＣカード１２から入力される問い合わせに対するレスポンス信号を、バス５５およびＳＣＣ５３を介して、パーソナルコンピュータ１４に出力し、パーソナルコンピュータ１４のＣＰＵは、リーダライタ１５から入力されたレスポンス、および、インターネット１１を介して、アクワイアラ・ブランドホルダ１から入力された売上承認要求に対するレスポンスを基に、コマンド処理は可能か否かを判断する。ステップＳ１３６において、コマンド処理ができないと判断された場合、処理は、ステップＳ１４４に進む。

【０２６８】

ステップＳ１３６において、コマンド処理が可能であると判断された場合、ステップＳ１３７において、リーダライタ１５のＤＰＵ５１は、ＩＣカード１２に対して価値充填処理を実行させる（ＩＣカード１２の対象となるファイルに記録されている電子マネーの値から、所定の値を減算する）ためのコマンドを生成して、バス５５を介してＳＰＵ５２に出力する。ＳＰＵ５２および変調回路４３において所定の処理が施されて、コマンドに対応する変調波が生成され、アンテナ

４６を介して、電磁波としてＩＣカード１２に送信される。

【０２６９】

ステップＳ１３８において、図１８のステップＳ９０と同様の処理が実行される。

【０２７０】

ステップＳ１３９において、リーダライタのＤＰＵ５１は、バス５５、ＳＣＣ５３、パーソナルコンピュータ１４、およびインターネット１１を介して、コマンド処理結果を、サイバー店舗１６に通知する。

【０２７１】

サイバー店舗１６の売上管理サーバ１９１は、ステップＳ１４０において、在庫／売上管理ＤＢ１９２を更新し、ステップＳ１４１において、ウェブサーバ１９３、およびインターネット１１を介して、アクワイアラ・ブランドホルダ１に処理結果を通知する。なお、コマンド処理結果の通知は、処理が行われる毎に逐次通知するようにしても良いし、例えば１週間や１ヶ月といった、所定の期間毎に行われるようにしても良い。

【０２７２】

ステップＳ１４２およびステップＳ１４３において、図１５のステップＳ３９およびステップＳ４０と同様の処理が実行される。

【０２７３】

ステップＳ１３２において、正しく認証されなかったと判断された場合、もしくは、ステップＳ１３６において、コマンド処理が可能ではないと判断された場合、ステップＳ１４４において、サイバー店舗１６の売上管理サーバ１９１は、ウェブサーバ１９３およびインターネット１１を介して、パーソナルコンピュータ１４に、エラーメッセージを出力する。

【０２７４】

ステップＳ１４５において、図１５のステップＳ４２と同様の処理が実行される。

【０２７５】

以上説明した処理においては、非接触ＩＣカードを用いた情報の授受が行われ

る場合について説明したが、利用者３が保有する、電子マネーなどの情報を記録し、各種処理を行うためのハードウェアは、例えば、接触型ＩＣカード、携帯電話、ＰＤＡ、パーソナルコンピュータ、時計などの、様々な情報処理機器が用いられるようにしても良い。

【０２７６】

上述した一連の処理は、ソフトウェアにより実行することもできる。そのソフトウェアは、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【０２７７】

この記録媒体は、図４、図７、あるいは図８に示すように、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク６５、１１１、もしくは１３１（フロッピーディスクを含む）、光ディスク６６、１１２、もしくは１３２（CD-ROM (Compact Disk-Read Only Memory)，DVD (Digital Versatile Disk) を含む）、光磁気ディスク６７、１１３、もしくは１３３（MD(Mini-Disk)を含む）、あるいは、半導体メモリ６８、１１４、もしくは１３４などよりなるパッケージメディアなどにより構成される。

【０２７８】

また、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０２７９】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０２８０】

【発明の効果】

本発明の情報処理装置、情報処理方法、および記録媒体に記録されているプログラムによれば、電子マネー情報、および電子マネーサービスに関する認証処理に用いられる認証情報が記録される第１の情報処理装置を発行する第２の事業者が管理する第２の情報処理装置と情報を授受し、電子マネーを利用したサービスを提供する第３の事業者が管理する第３の情報処理装置と情報を授受し、電子マネーサービスに関する認証処理に用いられる認証情報を記録し、第２の事業者に関する情報、および第１の事業者と第２の事業者との提携内容に関する情報を記録し、第３の事業者に関する情報、および第１の事業者と第３の事業者との提携内容に関する情報を記録し、第１の事業者と第２の事業者との提携内容に関する情報に基づいて、認証情報を出力し、第１の事業者と第３の事業者との提携内容に関する情報に基づいて、認証情報を出力するようにしたので、電子マネー事業において、１つのブランドを管理する事業体が管理する情報処理装置において、イシュアおよび加盟店に対する暗号鍵の配布、およびシステムの運営・管理を一元化し、事業体として必要なコストを低減することができる。

【０２８１】

本発明の電子マネーサービス提供システムによれば、第１の情報処理装置で、第２の事業者が管理する第３の情報処理装置と情報を授受し、第３の事業者が管理する第４の情報処理装置と情報を授受し、電子マネーサービスに関する認証処理に用いられる認証情報を記録し、第２の事業者に関する情報、および第１の事業者と第２の事業者との提携内容に関する情報を記録し、第３の事業者に関する情報、および第１の事業者と第３の事業者との提携内容に関する情報を記録し、第１の事業者と第２の事業者との提携内容に関する情報に基づいて、認証情報を出力し、第１の事業者と第３の事業者との提携内容に関する情報に基づいて、認証情報を出力し、第２の情報処理装置で、認証情報を記録し、電子マネー情報を記録し、第３の情報処理装置で、第１の情報処理装置と情報を授受し、入力された認証情報を記録し、第２の情報処理装置の発行に関する情報を記録し、記録された認証情報に基づいて、第２の情報処理装置との認証処理を実行し、第４の情報処理装置で、第１の情報処理装置と情報を授受し、入力された認証情報を記録し、記録された認証情報に基づいて、第２の情報処理装置との認証処理を実行す

るようにしたので、電子マネー事業において、１つのブランドに対して、多くのイシュアおよび加盟店が参画することができ、イシュアおよび加盟店に対する暗号鍵の配布、およびシステムの運営・管理に必要となるコストを低減することができる。

【図面の簡単な説明】

【図１】

本発明を適応した電子マネーサービス提供システムの構成を説明するための図である。

【図２】

電子マネーサービス提供システムにおけるネットワーク接続の構成、および、アクワイアラ・ブランドホルダによる鍵の発行について説明するための図である。

【図３】

ＩＣカード、リーダライタ、およびコントローラについて説明するための図である。

【図４】

図３のリーダライタの構成を示すブロック図である。

【図５】

図３のＩＣカードの構成を示すブロック図である。

【図６】

図５のEEPROMの論理フォーマットについて説明するための図である。

【図７】

図３のコントローラの構成を示すブロック図である。

【図８】

図２のパーソナルコンピュータの構成を示すブロック図である。

【図９】

アクワイアラ・ブランドホルダの構成を示すブロック図である。

【図１０】

イシュアの構成を示すブロック図である。

【図１１】

イシュアの構成を示すブロック図である。

【図１２】

入金端末装置もしくはＭＭＫにおいて電子マネーの充填処理を実行するための鍵の配置について説明するための図である。

【図１３】

入金端末装置もしくはＭＭＫにおける電子マネーの充填処理について説明するためのフローチャートである。

【図１４】

インターネットを介した電子マネーの充填処理を実行するための鍵の配置について説明するための図である。

【図１５】

インターネットを介した電子マネーの充填処理について説明するためのフローチャートである。

【図１６】

インターネットを介した電子マネーの充填処理をアクワイアラ・ブランドホルダが代行する場合の処理について説明するためのフローチャートである。

【図１７】

店舗において、ＩＣカードを用いた商品、もしくはサービスの購入処理を可能とするための鍵の配置について説明するための図である。

【図１８】

店舗における、ＩＣカードを用いた商品、もしくはサービスの購入処理について説明するためのフローチャートである。

【図１９】

店舗における、ＩＣカードを用いた商品、もしくはサービスの購入処理について説明するためのフローチャートである。

【図２０】

サイバー店舗において、ＩＣカードを用いた商品、もしくはサービスの購入処理を可能とするための鍵の配置について説明するための図である。

【図２１】

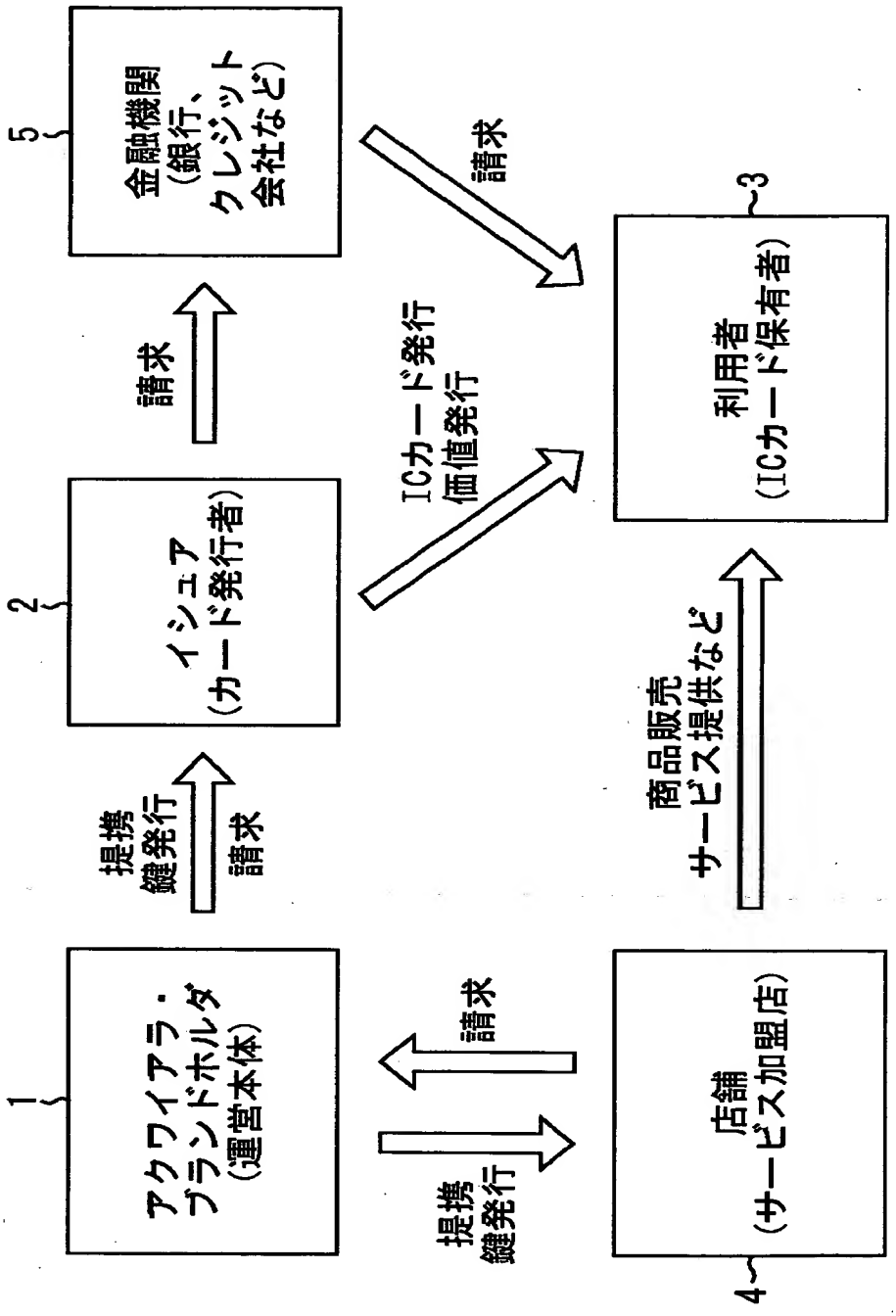
サイバー店舗における、ＩＣカードを用いた商品、もしくはサービスの購入処理について説明するためのフローチャートである。

【符号の説明】

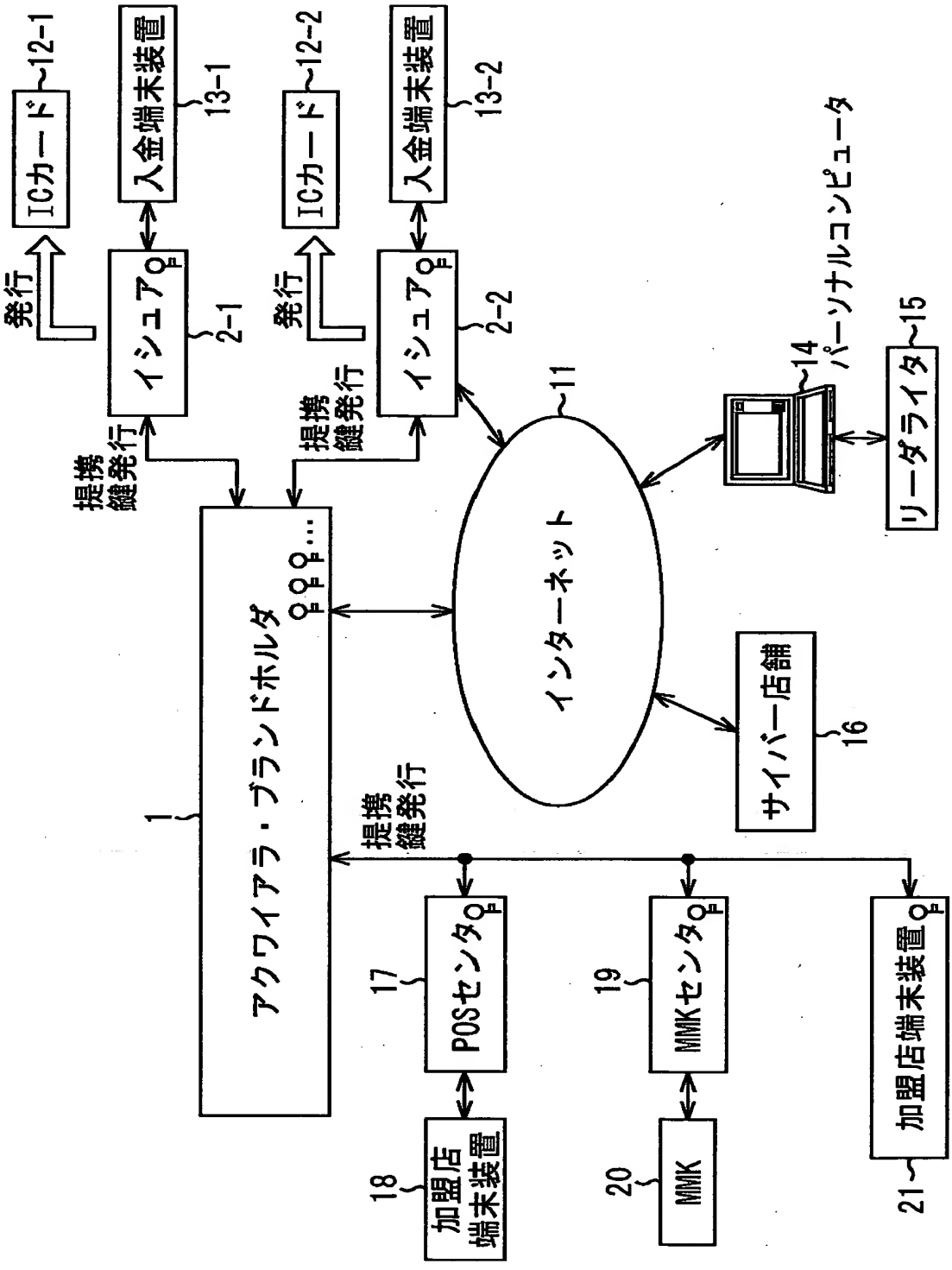
１　アクワイアラ・ブランドホルダ、　２　イシュア、　４　店舗、　１１　インターネット、　１２　ＩＣカード、　１３　入金端末装置、　１４　パーソナルコンピュータ、　１５　リーダライタ、　１６　サイバー店舗、　１７　ＰＯＳセンタ、　１８　加盟店端末装置、　１９　ＭＭＫセンタ、　２０　ＭＭＫ，　２１　加盟店端末装置、　３１　リーダライタ、　３２　コントローラ、　１４１　店舗管理サーバ、　１４２　店舗管理ＤＢ、　１４３　顧客サーバ、　１４４　顧客ＤＢ、　１４５　セキュリティサーバ　１４６　鍵管理ＤＢ、　１４７　課金サーバ、　１４８　入金代行ＤＢ、　１４９　店舗Ｇ／Ｗサーバ、　１５０　ウェブサーバ、　１５１　イシュアＧ／Ｗサーバ

【書類名】図面

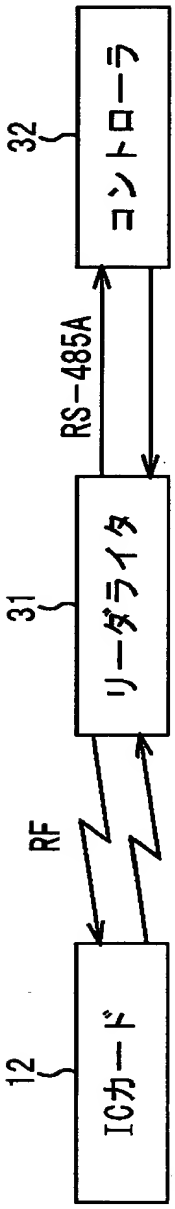
【図１】


1
アクワイアラ・
ブランドホルダ
(運営本体)
2
イシュア
(カード発行者)
3
利用者
(ICカード保有者)
4
店舗
(サービス加盟店)
5
金融機関
(銀行、
クレジット
会社など)
提携
鍵発行
請求
請求
提携
鍵発行
請求
ICカード発行
価値発行
請求
商品販売
サービス提供など

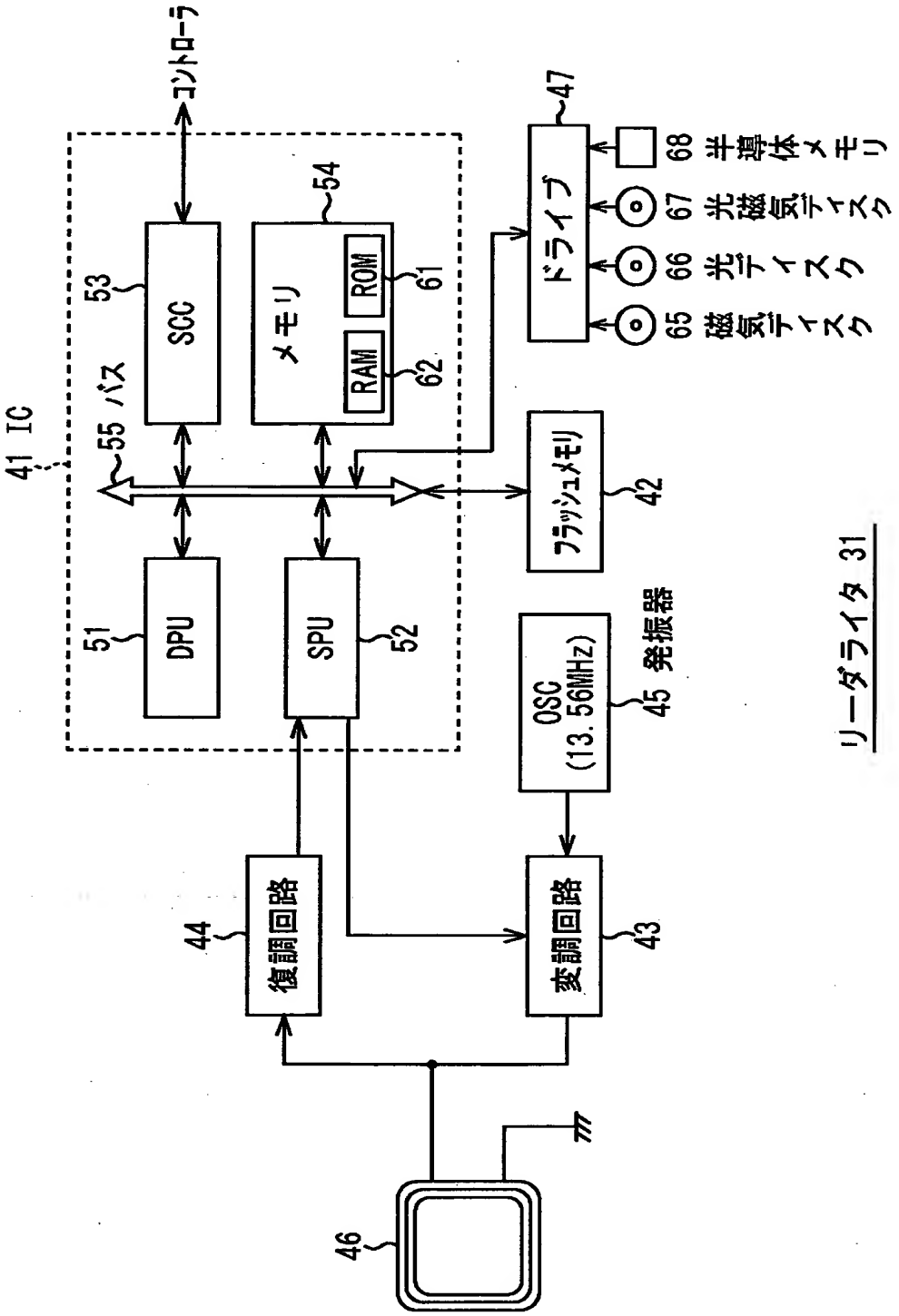
【図２】


ICカード
12-1
入金端末装置
13-1
ICカード
12-2
入金端末装置
13-2
発行
発行
イシュア
2-1
イシュア
2-2
提携鍵発行
提携鍵発行
11
インターネット
パーソナルコンピュータ
14
リーダライタ
15
アクワイアラ・ブランドホルダ
1
提携鍵発行
サイバー店舗
16
POSセンタ
17
MMKセンタ
19
加盟店端末装置
21
加盟店端末装置
18
MMK
20

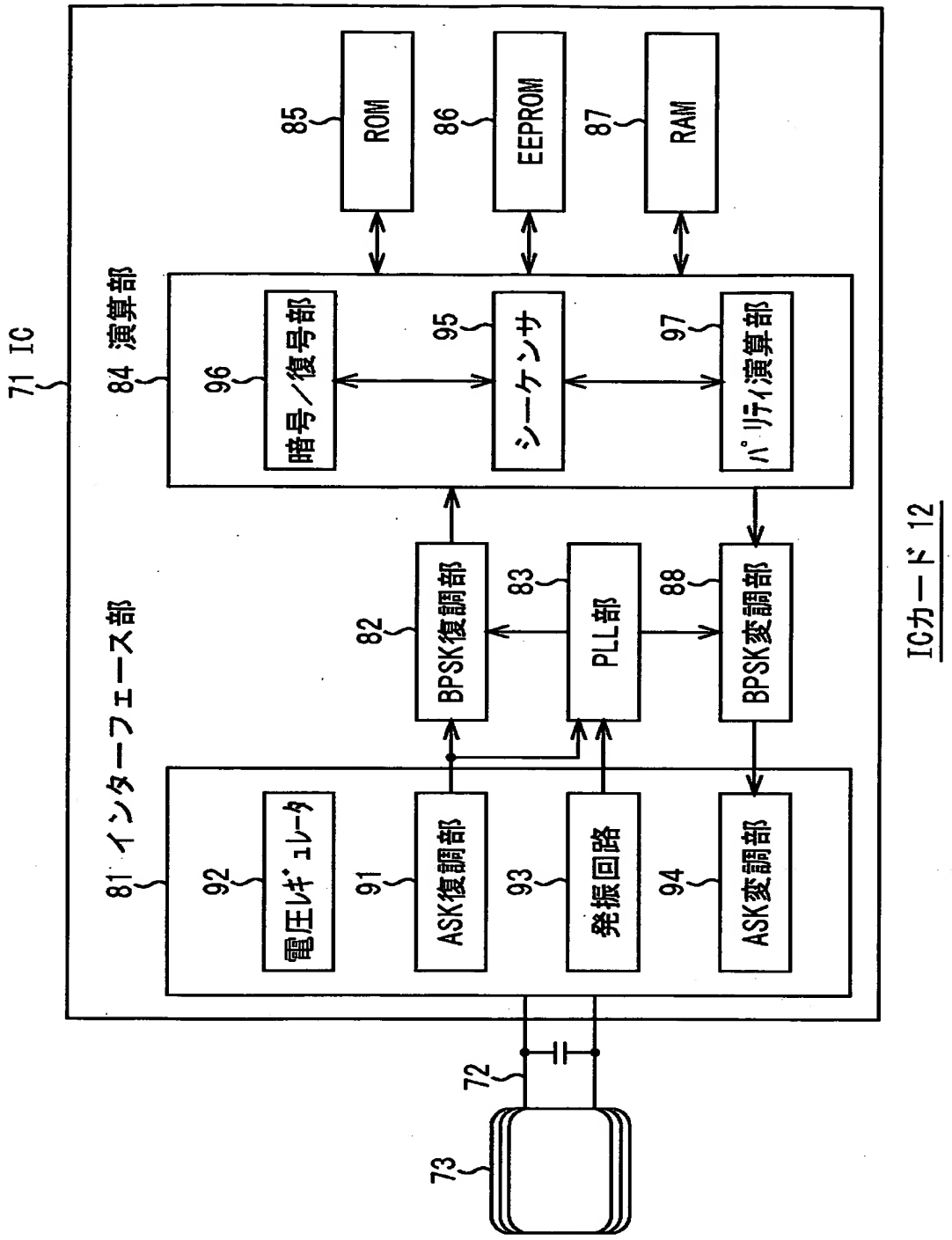
【図３】



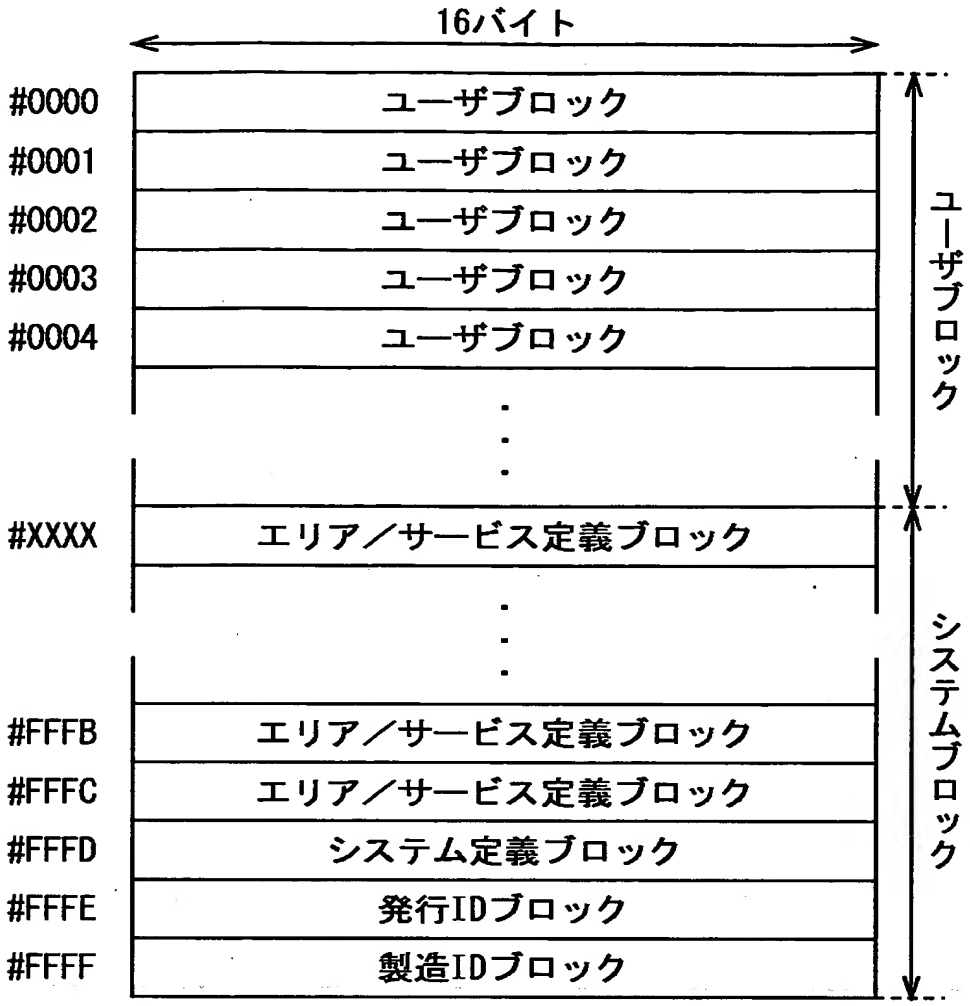
【図４】


コントローラ
47
ドライブ
68 半導体メモリ
67 光磁気ディスク
66 光ディスク
65 磁気ディスク
54
メモリ
ROM
61
RAM
62
53
SCC
41 IC
55 バス
フラッシュメモリ
42
51
DPU
SPU
52
OSC
(13.56MHz)
45 発振器
リーダライタ 31
44
復調回路
変調回路
43
46

【図５】

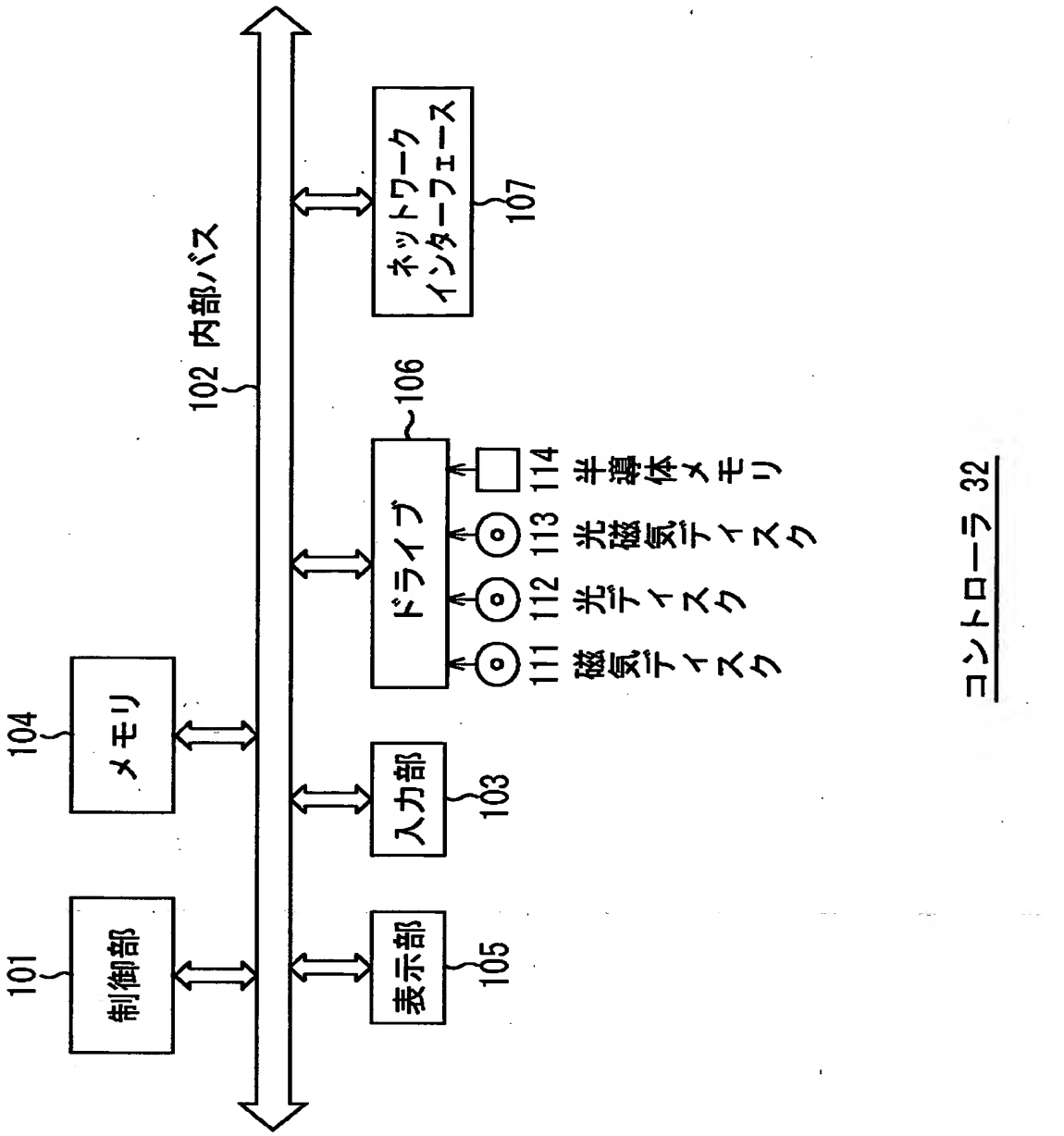

71 IC
81 インターフェース部
84 演算部
85 ROM
86 EEPROM
87 RAM
96 暗号／復号部
95 シーケンサ
97 パリティ演算部
82 BPSK復調部
83 PLL部
88 BPSK変調部
92 電圧レギュレータ
91 ASK復調部
93 発振回路
94 ASK変調部
72
73
ICカード 12

【図６】

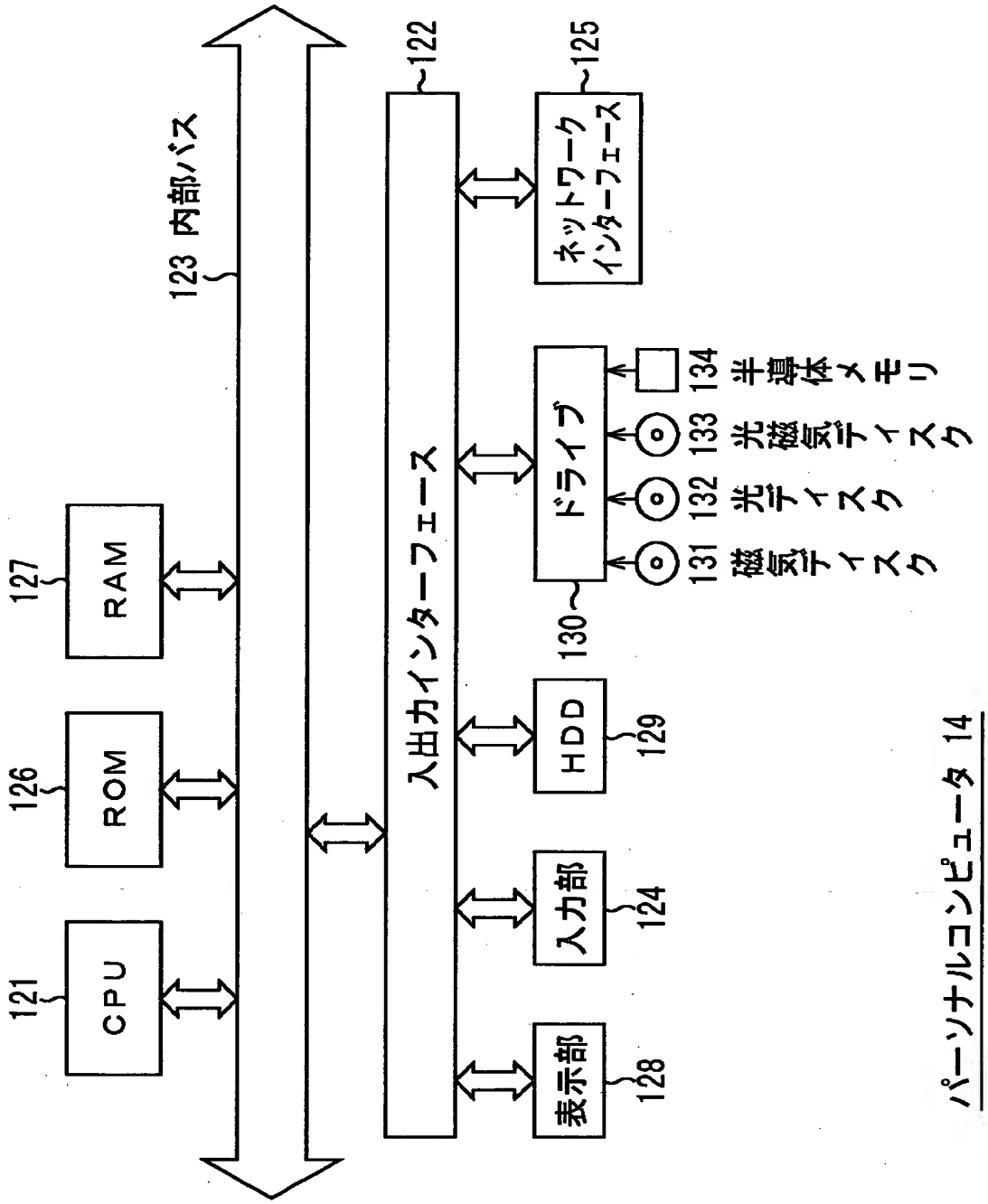


EEPROM86の論理フォーマット

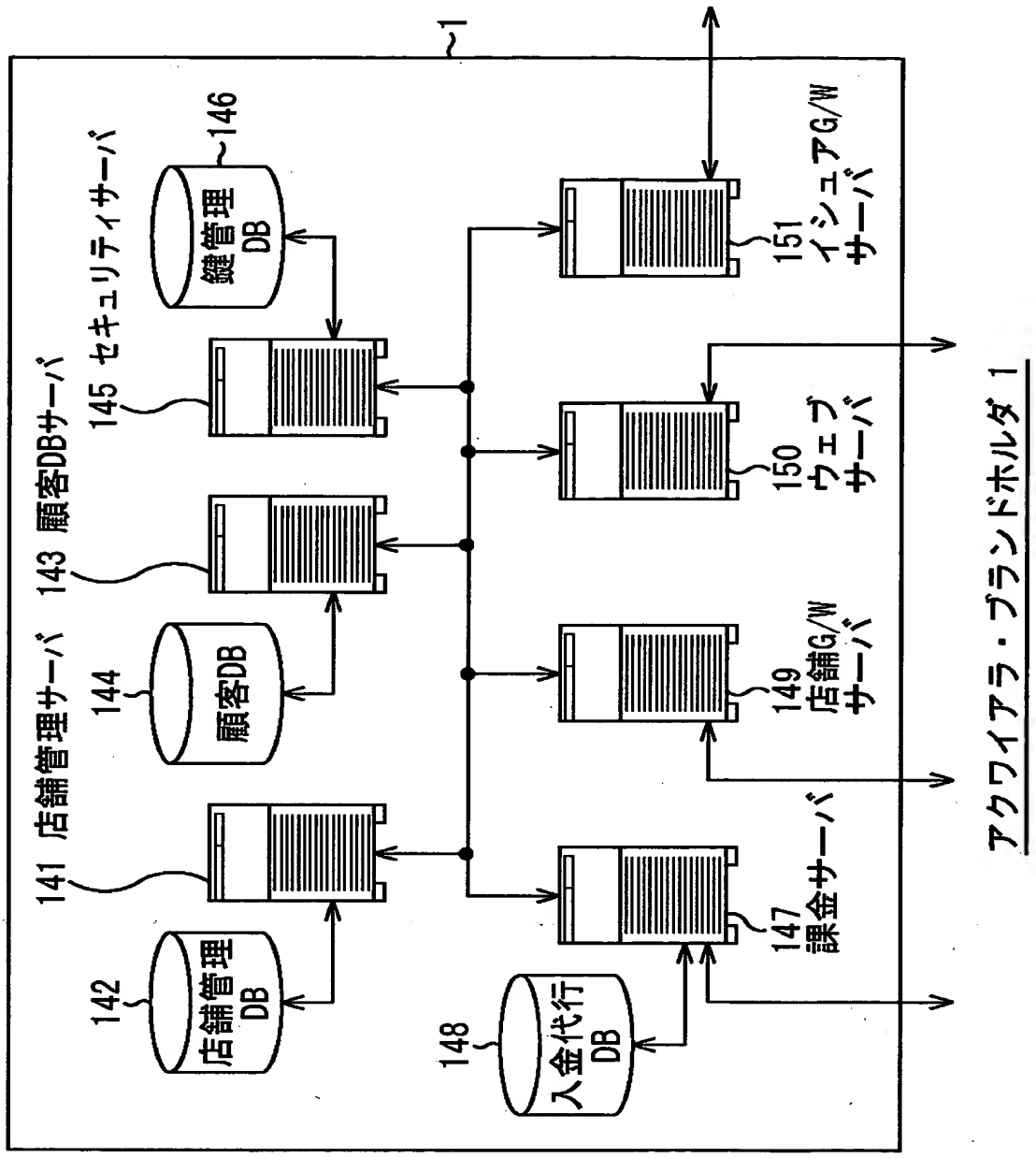
【図７】


101 制御部
104 メモリ
102 内部バス
103 入力部
105 表示部
106 ドライブ
111 磁気ディスク
112 光ディスク
113 光磁気ディスク
114 半導体メモリ
107 ネットワークインターフェース
コントローラ 32

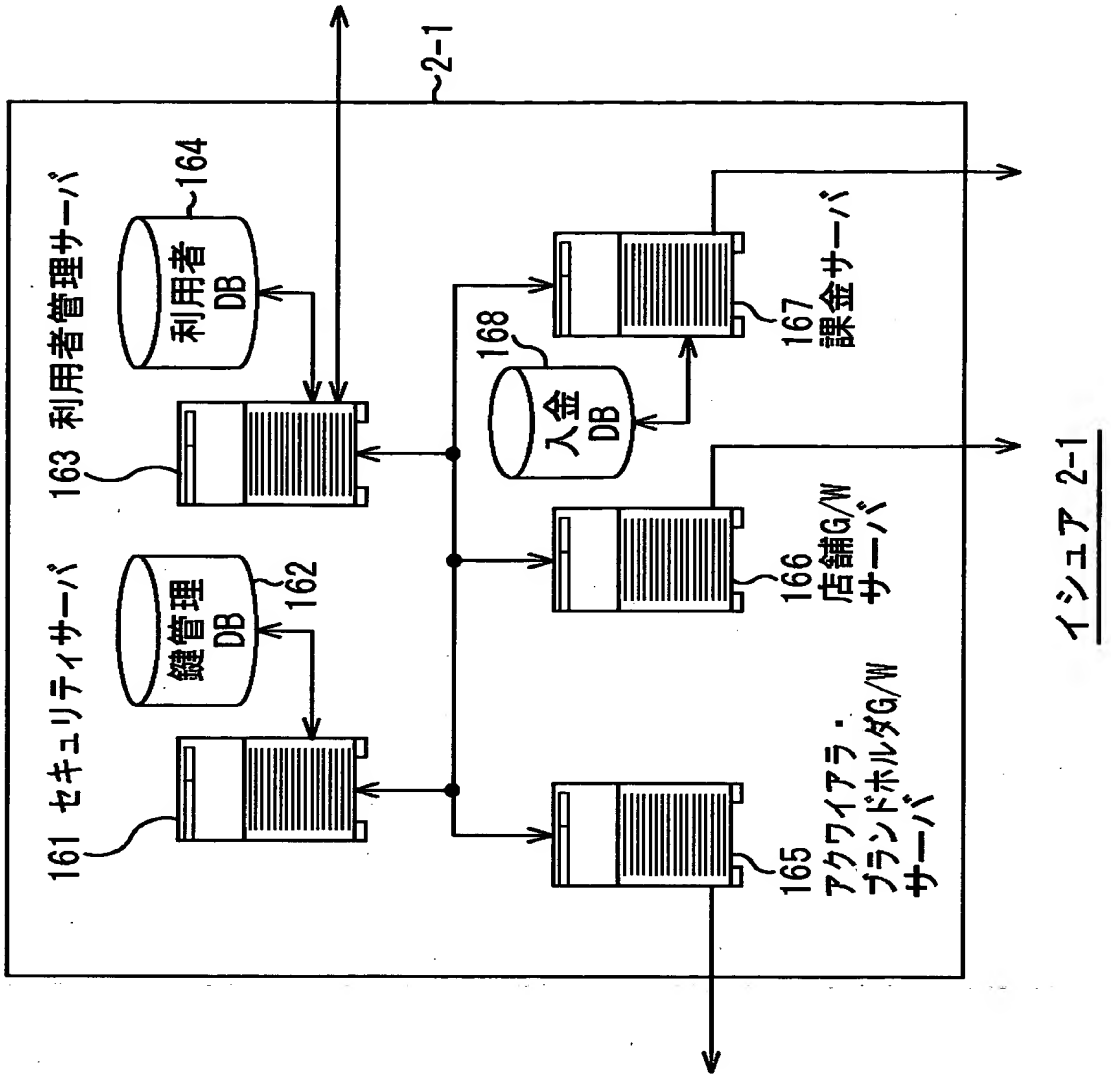
【図８】


パーソナルコンピュータ 14
CPU
121
ROM
126
RAM
127
123 内部バス
入出力インターフェース
122
入力部
124
表示部
128
HDD
129
ドライブ
130
131 磁気ディスク
132 光ディスク
133 光磁気ディスク
134 半導体メモリ
ネットワーク
インターフェース
125

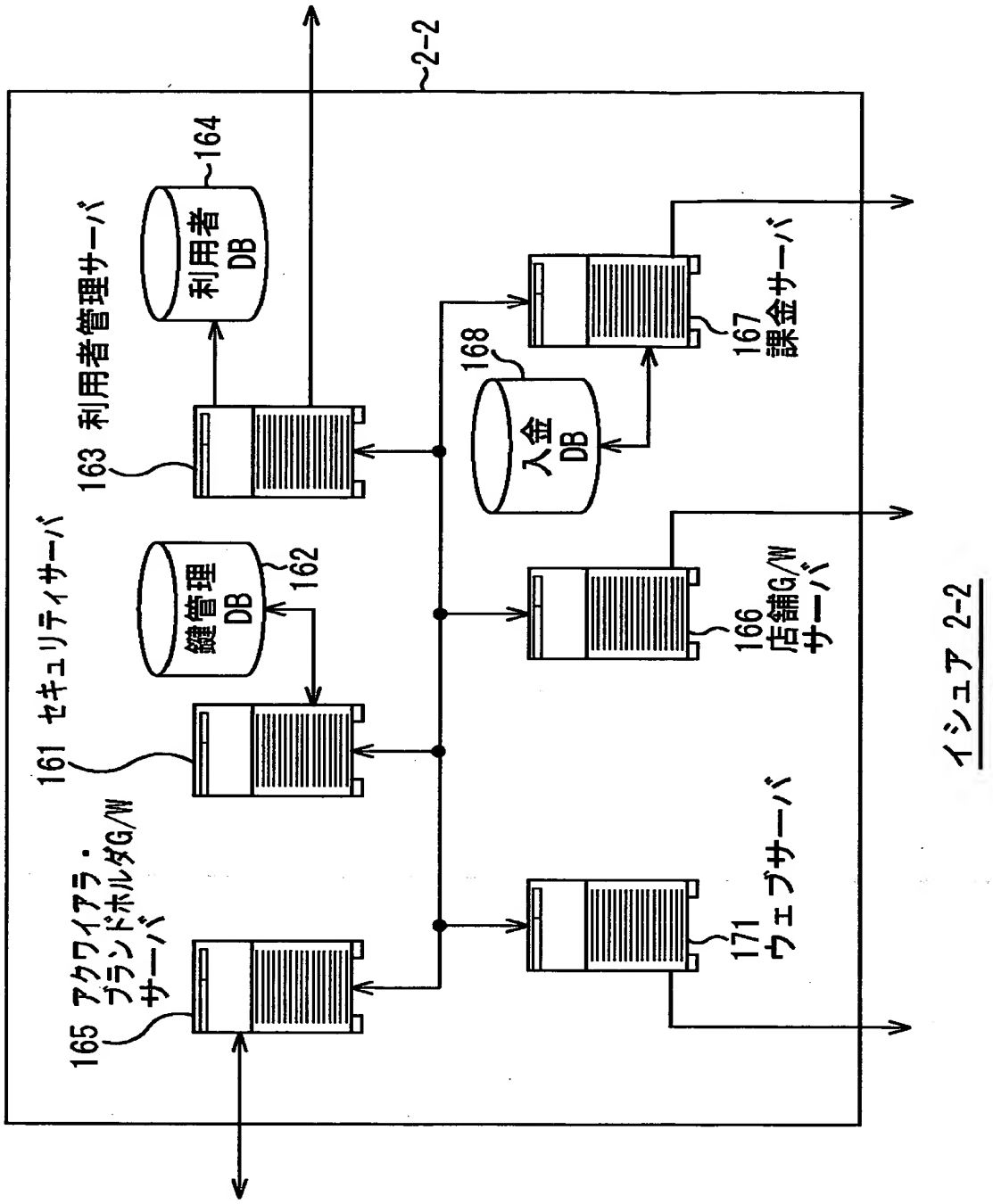
【図９】


1
141 店舗管理サーバ
142 店舗管理DB
143 顧客DBサーバ
144 顧客DB
145 セキュリティサーバ
146 鍵管理DB
147 課金サーバ
148 入金代行DB
149 店舗G/Wサーバ
150 ウェブサーバ
151 イシュアG/Wサーバ
アクワイアラ・ブランドホルダ 1

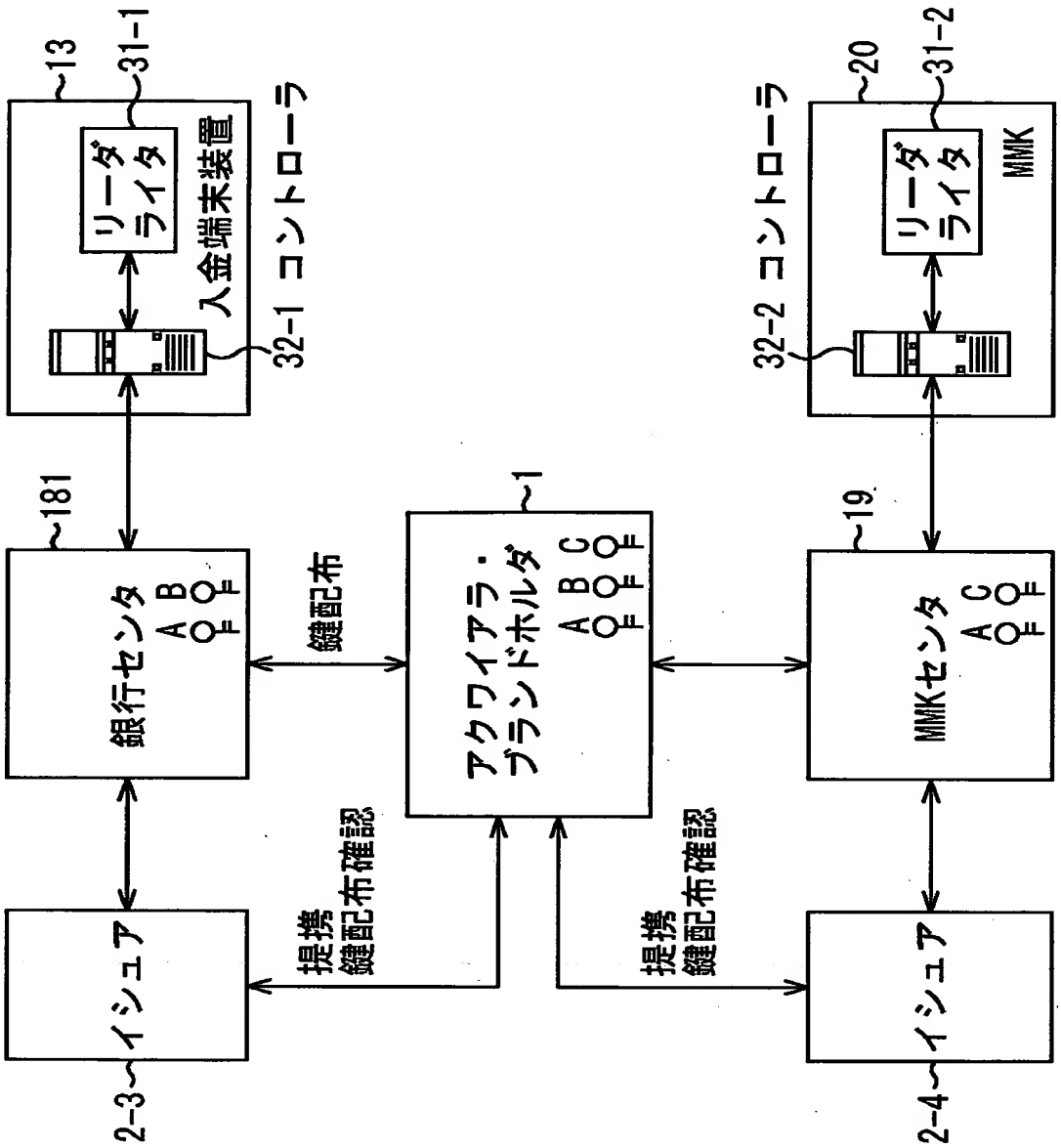
【図１０】


2-1
164
利用者DB
163 利用者管理サーバ
168
入金DB
167
課金サーバ
162
鍵管理DB
161 セキュリティサーバ
166
店舗G/W
サーバ
165
アクワイアラ・
ブランドホルダG/W
サーバ
イシュア 2-1

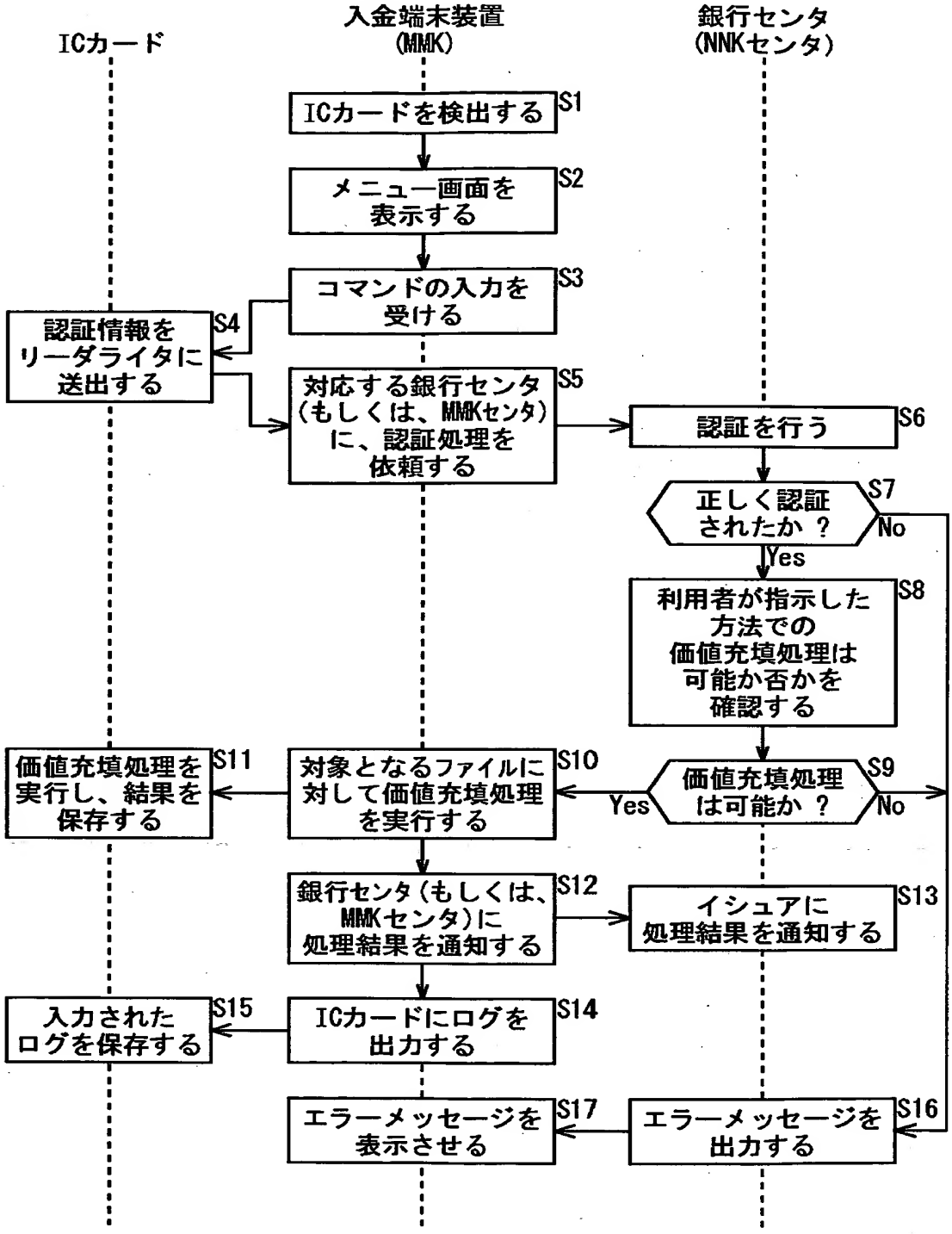
【図１１】


2-2
164
利用者DB
163 利用者管理サーバ
168
入金DB
167 課金サーバ
162
鍵管理DB
161 セキュリティサーバ
166 店舗G/Wサーバ
165 アクワイアラ・ブランドホルダG/Wサーバ
171 ウェブサーバ
イシュア 2-2

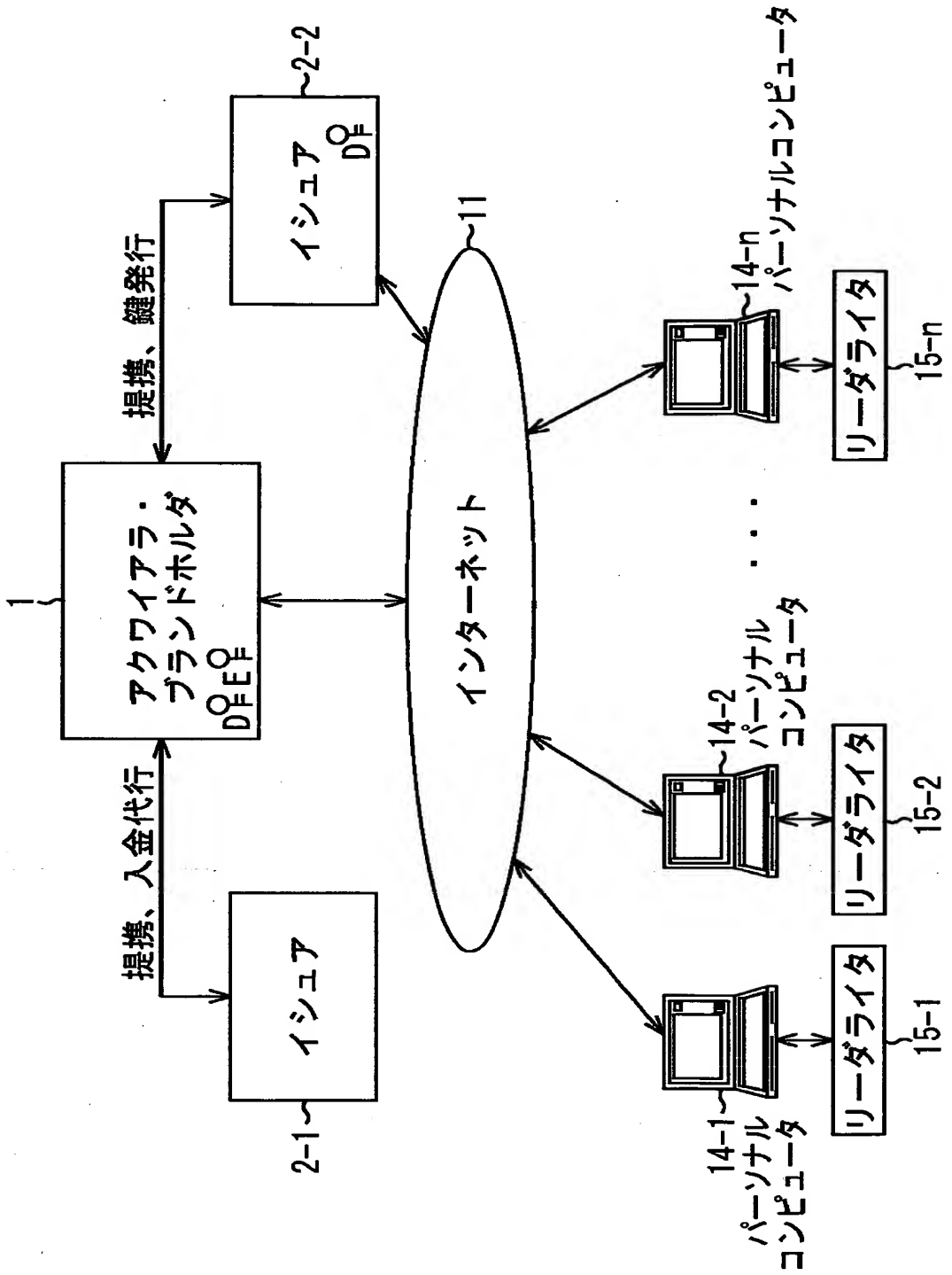
【図１２】


13
31-1
リーダ ライタ
入金端末装置
32-1 コントローラ
181
銀行センタ
A B
O F
鍵配布
1
アクワイアラ・
ブランドホルダ
A B C
O F
19
MMKセンタ
A C
O F
20
31-2
リーダ ライタ
MMK
32-2 コントローラ
提携
鍵配布確認
提携
鍵配布確認
イシュア
2-3
イシュア
2-4

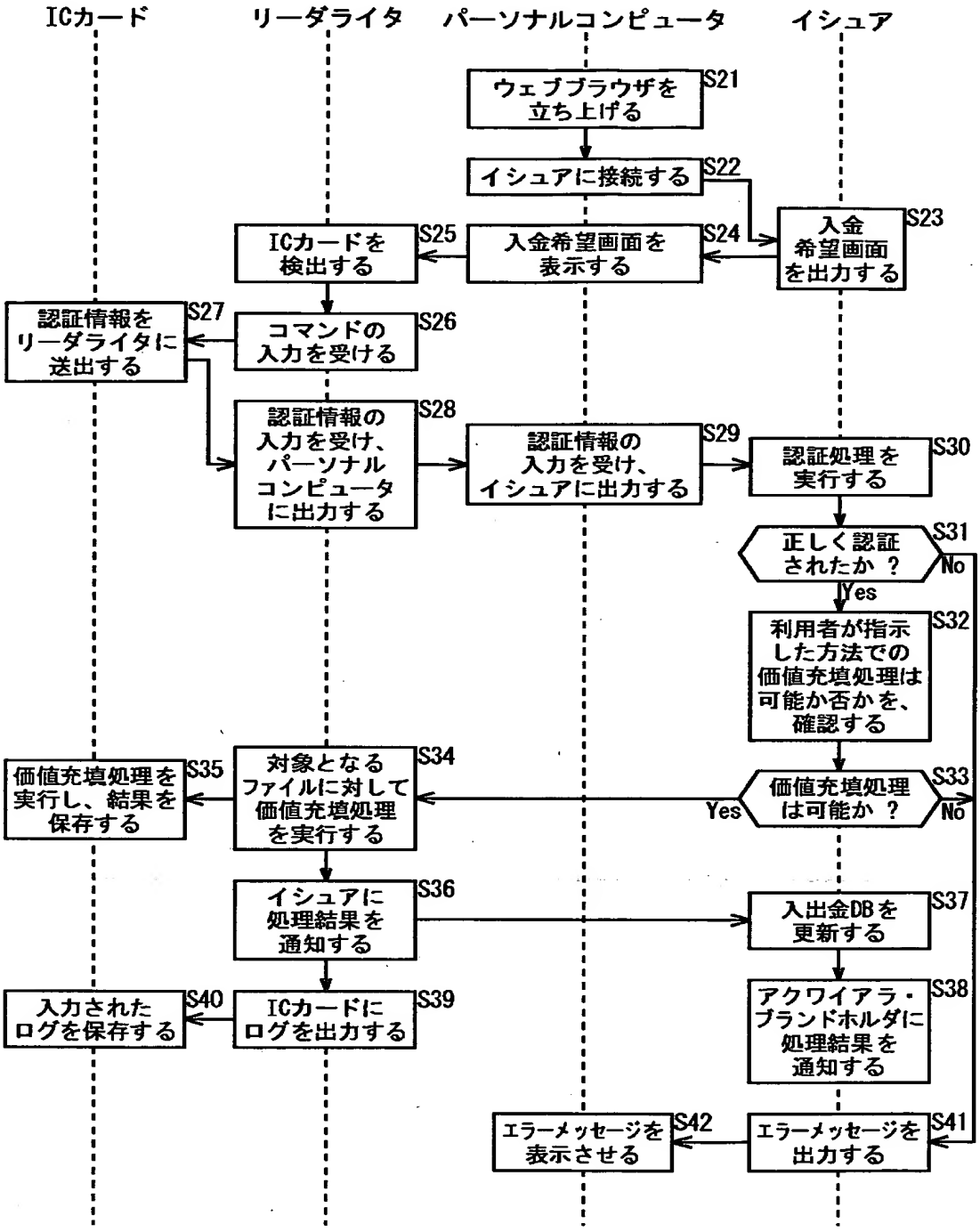
【図１３】


ICカード
入金端末装置
(MMK)
銀行センタ
(NNKセンタ)
ICカードを検出する
S1
メニュー画面を
表示する
S2
コマンドの入力を
受ける
S3
認証情報を
リーダライタに
送出する
S4
対応する銀行センタ
(もしくは、MMKセンタ)
に、認証処理を
依頼する
S5
認証を行う
S6
正しく認証
されたか ？
S7
No
Yes
利用者が指示した
方法での
価値充填処理は
可能か否かを
確認する
S8
価値充填処理
は可能か ？
S9
Yes
No
対象となるファイルに
対して価値充填処理
を実行する
S10
価値充填処理を
実行し、結果を
保存する
S11
銀行センタ(もしくは、
MMKセンタ)に
処理結果を通知する
S12
イシュアに
処理結果を通知する
S13
ICカードにログを
出力する
S14
入力された
ログを保存する
S15
エラーメッセージを
出力する
S16
エラーメッセージを
表示させる
S17

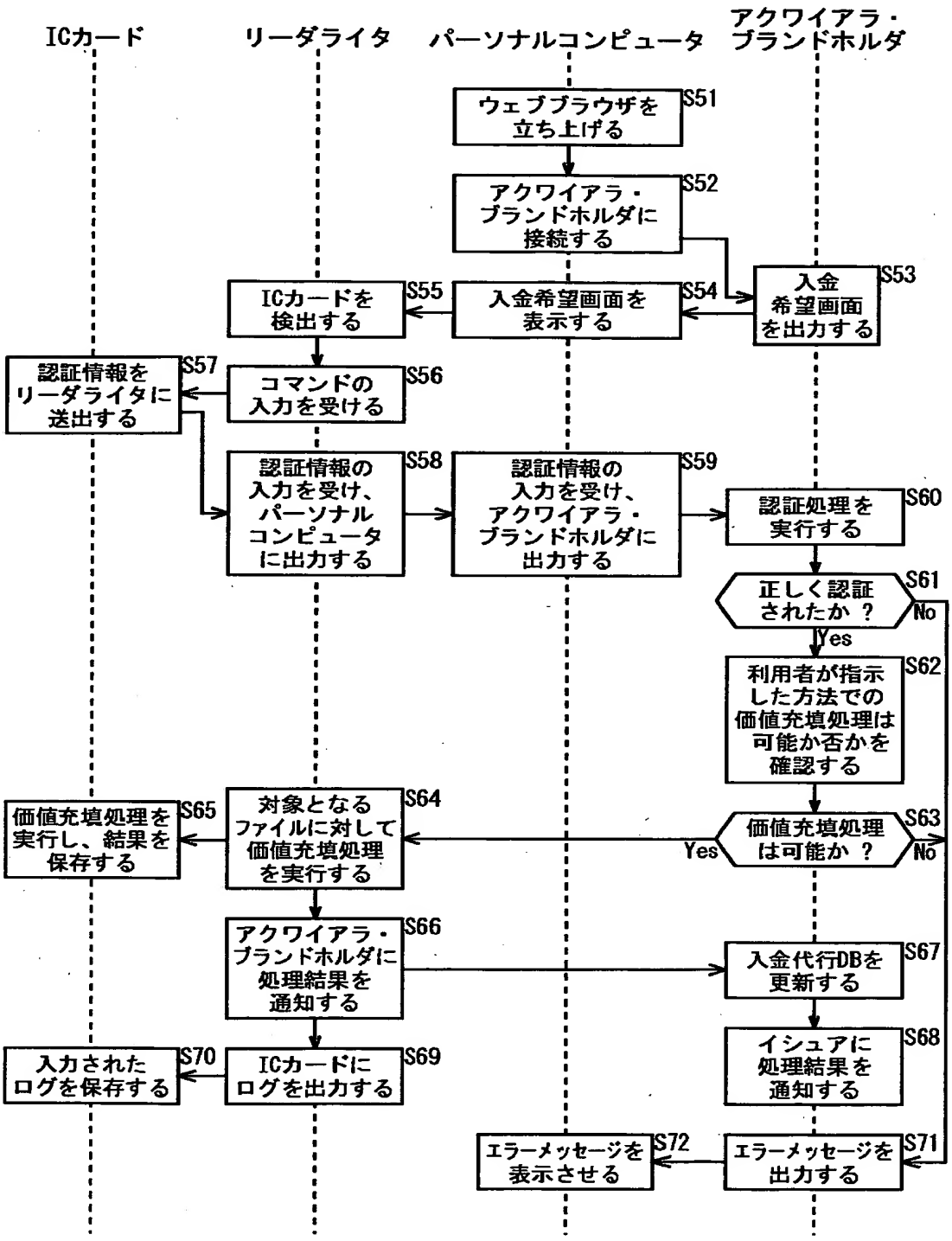
【図１４】


1
アクワイアラ・
ブランドホルダ
DFEPF
提携、鍵発行
提携、入金代行
イシュア
DPF
2-2
イシュア
2-1
インターネット
11
パーソナルコンピュータ
14-n
リーダライタ
15-n
パーソナル
コンピュータ
14-2
リーダライタ
15-2
パーソナル
コンピュータ
14-1
リーダライタ
15-1

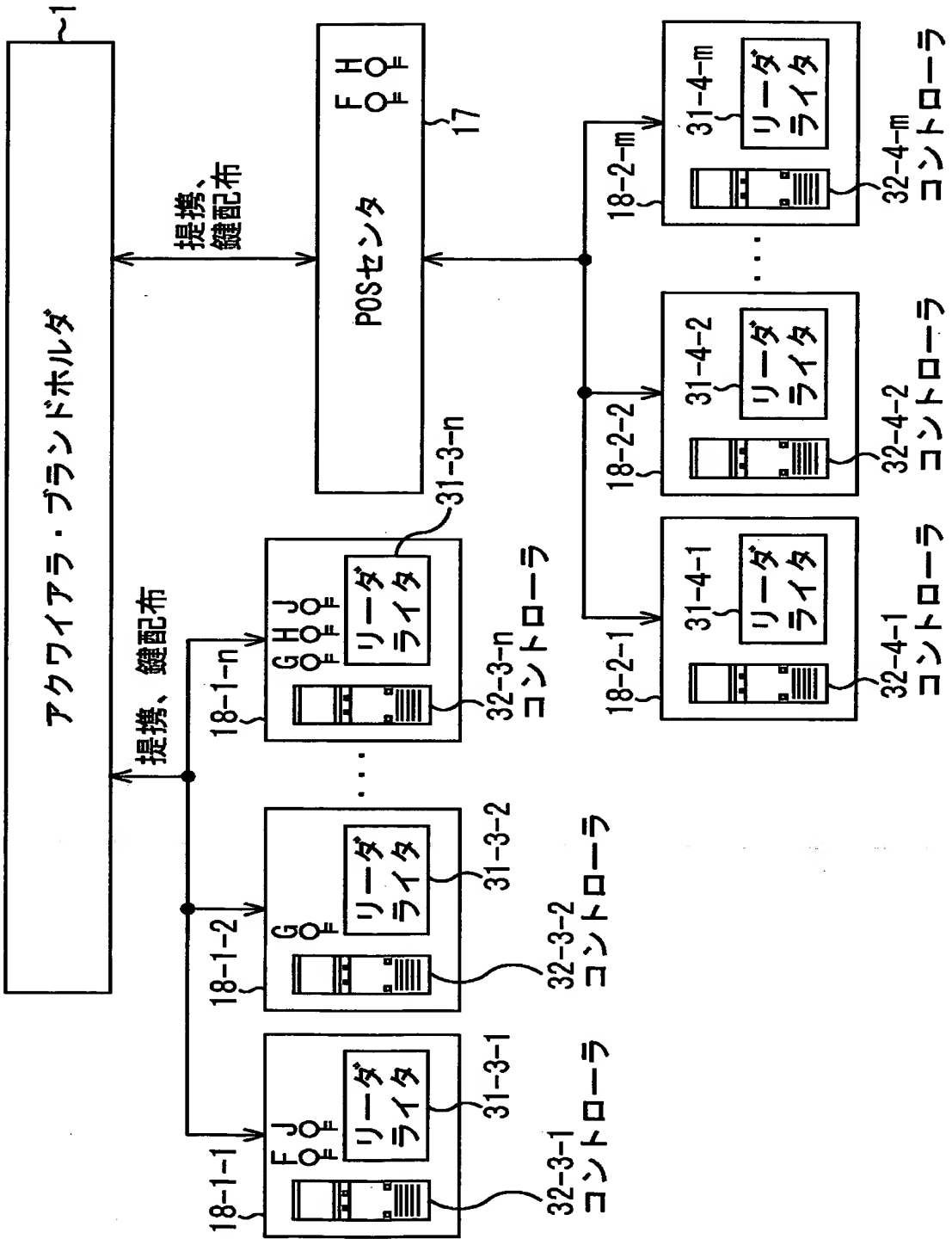
【図１５】


ICカード
リーダライタ
パーソナルコンピュータ
イシュア
ウェブブラウザを立ち上げる
S21
イシュアに接続する
S22
入金希望画面を出力する
S23
入金希望画面を表示する
S24
ICカードを検出する
S25
コマンドの入力を受ける
S26
認証情報をリーダライタに送出する
S27
認証情報の入力を受け、パーソナルコンピュータに出力する
S28
認証情報の入力を受け、イシュアに出力する
S29
認証処理を実行する
S30
正しく認証されたか？
S31
No
Yes
利用者が指示した方法での価値充填処理は可能か否かを、確認する
S32
価値充填処理は可能か？
S33
Yes
No
対象となるファイルに対して価値充填処理を実行する
S34
価値充填処理を実行し、結果を保存する
S35
イシュアに処理結果を通知する
S36
入出金DBを更新する
S37
アクワイアラ・ブランドホルダに処理結果を通知する
S38
ICカードにログを出力する
S39
入力されたログを保存する
S40
エラーメッセージを出力する
S41
エラーメッセージを表示させる
S42

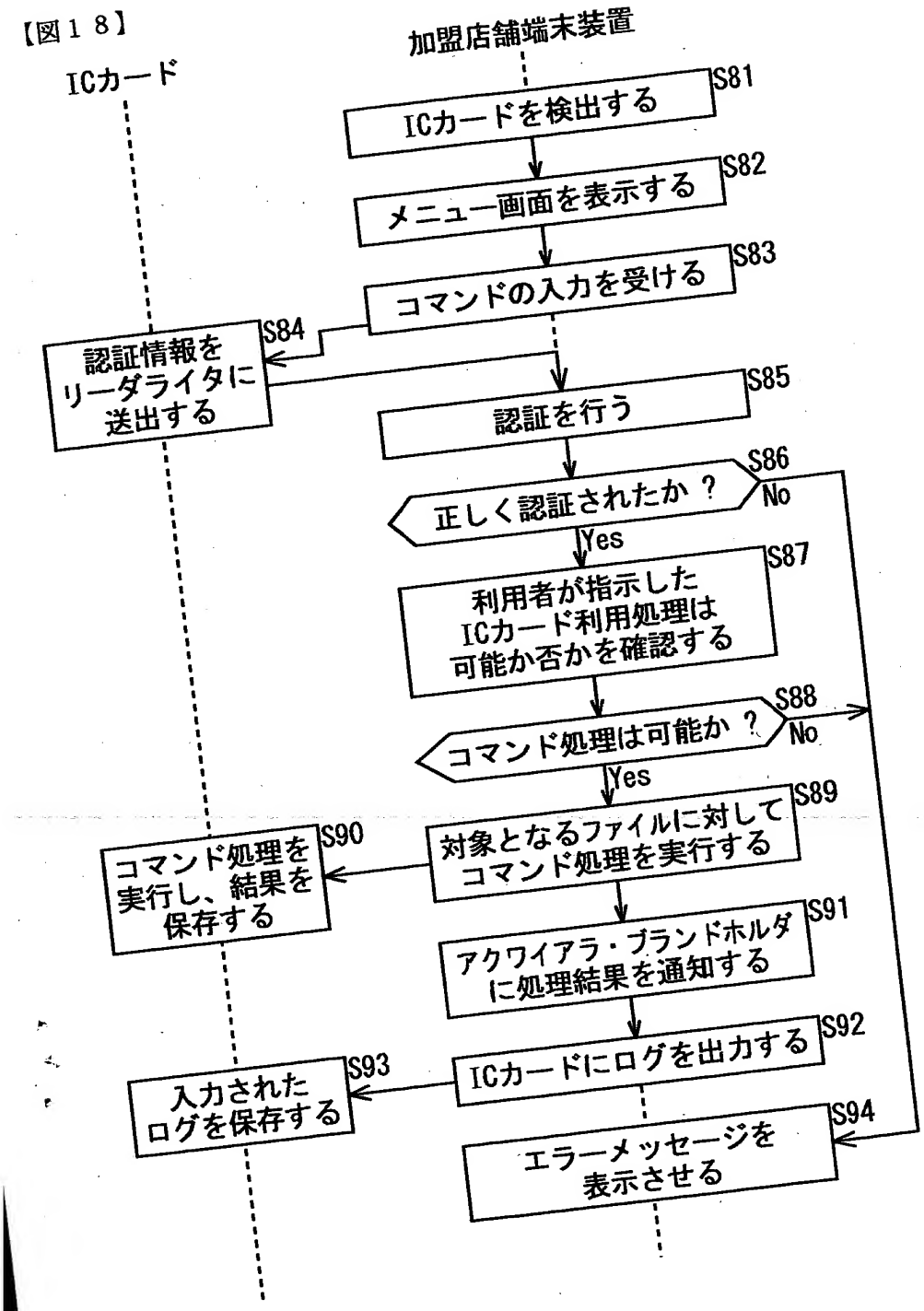
【図１６】


ICカード
リーダライタ
パーソナルコンピュータ
アクワイアラ・ブランドホルダ
ウェブブラウザを立ち上げる
S51
アクワイアラ・ブランドホルダに接続する
S52
入金希望画面を出力する
S53
入金希望画面を表示する
S54
ICカードを検出する
S55
コマンドの入力を受ける
S56
認証情報をリーダライタに送出する
S57
認証情報の入力を受け、パーソナルコンピュータに出力する
S58
認証情報の入力を受け、アクワイアラ・ブランドホルダに出力する
S59
認証処理を実行する
S60
正しく認証されたか？
S61
No
Yes
利用者が指示した方法での価値充填処理は可能か否かを確認する
S62
価値充填処理は可能か？
S63
Yes
No
対象となるファイルに対して価値充填処理を実行する
S64
価値充填処理を実行し、結果を保存する
S65
アクワイアラ・ブランドホルダに処理結果を通知する
S66
入金代行DBを更新する
S67
イシュアに処理結果を通知する
S68
ICカードにログを出力する
S69
入力されたログを保存する
S70
エラーメッセージを出力する
S71
エラーメッセージを表示させる
S72

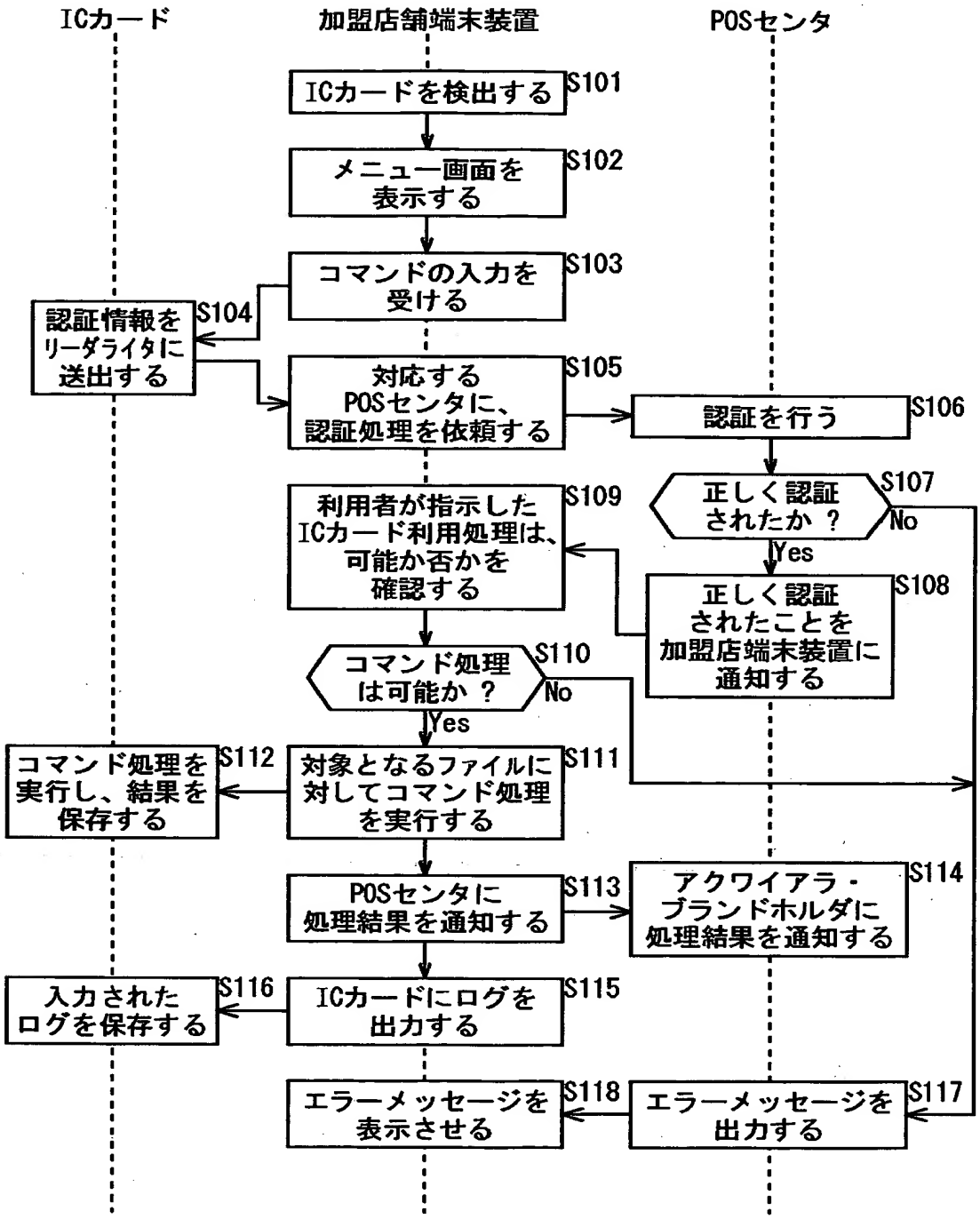
【図１７】


1
アクワイアラ・ブランドホルダ
提携、鍵配布
提携、鍵配布
POSセンタ
17
18-1-1
18-1-2
18-1-n
18-2-1
18-2-2
18-2-m
31-3-1
31-3-2
31-3-n
31-4-1
31-4-2
31-4-m
リーダライタ
32-3-1 コントローラ
32-3-2 コントローラ
32-3-n コントローラ
32-4-1 コントローラ
32-4-2 コントローラ
32-4-m コントローラ

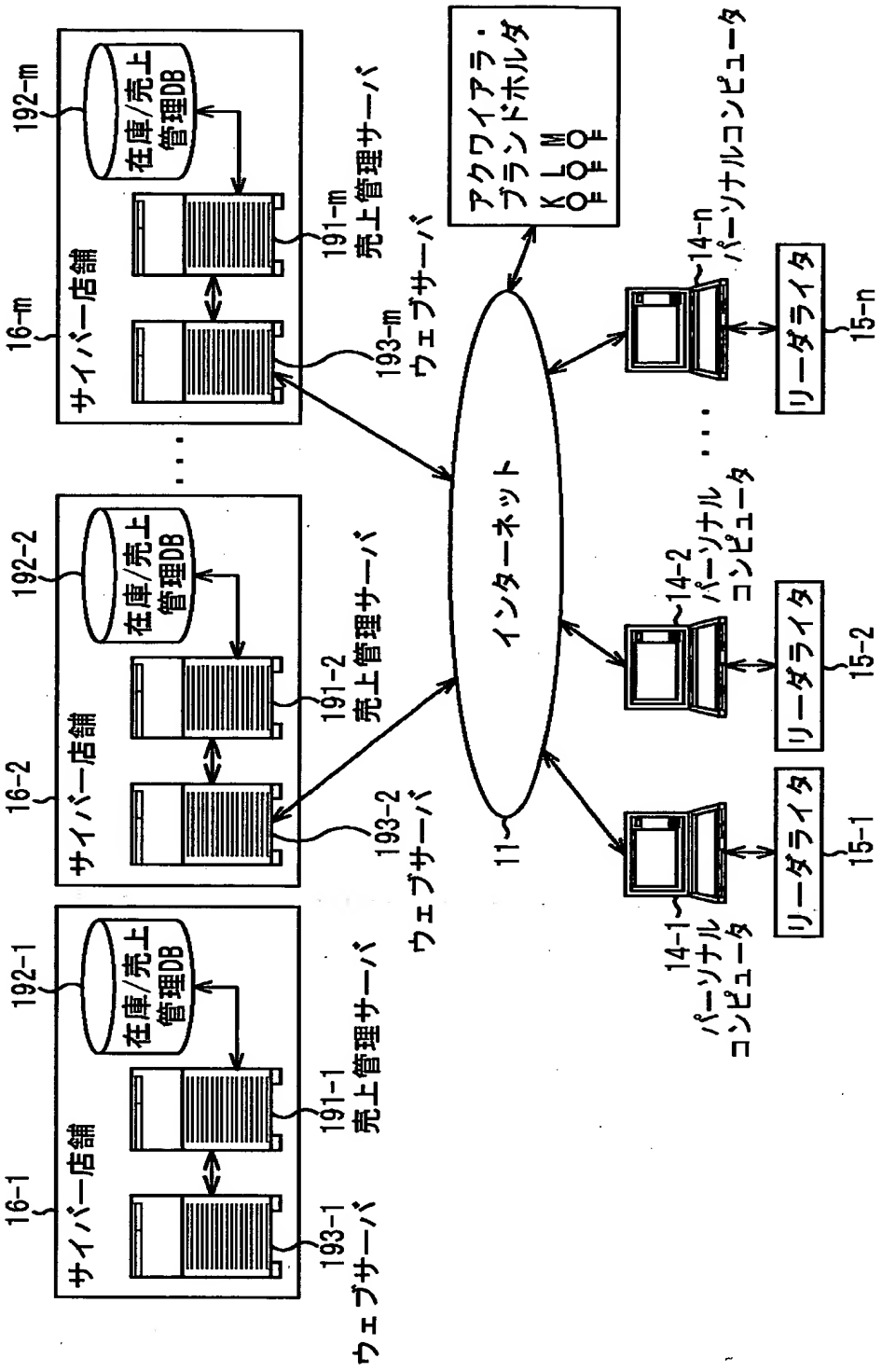
【図１８】


ICカード
加盟店舗端末装置
ICカードを検出する
S81
メニュー画面を表示する
S82
コマンドの入力を受ける
S83
認証情報をリーダライタに送出する
S84
認証を行う
S85
正しく認証されたか？
S86
No
Yes
利用者が指示したICカード利用処理は可能か否かを確認する
S87
コマンド処理は可能か？
S88
No
Yes
対象となるファイルに対してコマンド処理を実行する
S89
コマンド処理を実行し、結果を保存する
S90
アクワイアラ・ブランドホルダに処理結果を通知する
S91
ICカードにログを出力する
S92
入力されたログを保存する
S93
エラーメッセージを表示させる
S94

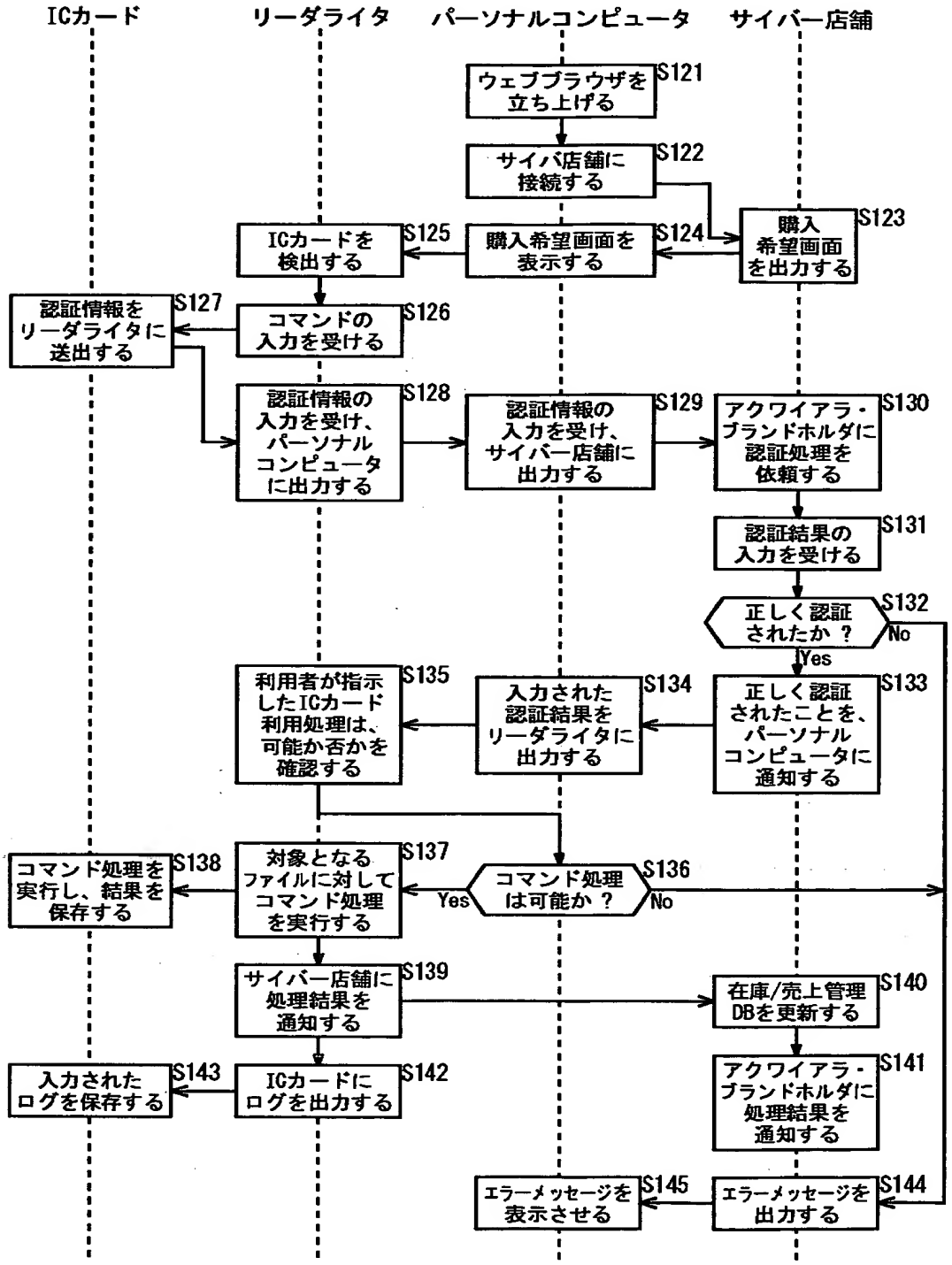
【図１９】


ICカード
加盟店舗端末装置
POSセンタ
ICカードを検出する
S101
メニュー画面を表示する
S102
コマンドの入力を受ける
S103
認証情報をリーダライタに送出する
S104
対応するPOSセンタに、認証処理を依頼する
S105
認証を行う
S106
正しく認証されたか ？
S107
No
Yes
利用者が指示したICカード利用処理は、可能か否かを確認する
S109
正しく認証されたことを加盟店端末装置に通知する
S108
コマンド処理は可能か ？
S110
No
Yes
コマンド処理を実行し、結果を保存する
S112
対象となるファイルに対してコマンド処理を実行する
S111
POSセンタに処理結果を通知する
S113
アクワイアラ・ブランドホルダに処理結果を通知する
S114
入力されたログを保存する
S116
ICカードにログを出力する
S115
エラーメッセージを表示させる
S118
エラーメッセージを出力する
S117

【図２０】


アクワイアラ・
ブランドホルダ
KLMOPF
インターネット
11
サイバー店舗
16-1
16-2
16-m
在庫/売上
管理DB
192-1
192-2
192-m
売上管理サーバ
191-1
191-2
191-m
ウェブサーバ
193-1
193-2
193-m
パーソナル
コンピュータ
14-1
14-2
14-n
リーダライタ
15-1
15-2
15-n

【図２１】


ICカード
リーダライタ
パーソナルコンピュータ
サイバー店舗
ウェブブラウザを立ち上げる
S121
サイバ店舗に接続する
S122
購入希望画面を出力する
S123
購入希望画面を表示する
S124
ICカードを検出する
S125
コマンドの入力を受ける
S126
認証情報をリーダライタに送出する
S127
認証情報の入力を受け、パーソナルコンピュータに出力する
S128
認証情報の入力を受け、サイバー店舗に出力する
S129
アクワイアラ・ブランドホルダに認証処理を依頼する
S130
認証結果の入力を受ける
S131
正しく認証されたか？
S132
No
Yes
正しく認証されたことを、パーソナルコンピュータに通知する
S133
入力された認証結果をリーダライタに出力する
S134
利用者が指示したICカード利用処理は、可能か否かを確認する
S135
コマンド処理は可能か？
S136
Yes
No
対象となるファイルに対してコマンド処理を実行する
S137
コマンド処理を実行し、結果を保存する
S138
サイバー店舗に処理結果を通知する
S139
在庫/売上管理DBを更新する
S140
アクワイアラ・ブランドホルダに処理結果を通知する
S141
ICカードにログを出力する
S142
入力されたログを保存する
S143
エラーメッセージを出力する
S144
エラーメッセージを表示させる
S145

【書類名】　　要約書

【要約】

【課題】　管理・運営費が安価で、自由度の高い電子マネーシステムを構築する。

【解決手段】　電子マネーのブランドを管理するアクワイアラ・ブランドホルダ１は、本システムの認証処理に用いられる鍵を全て管理し、必要に応じて鍵を発行する。アクワイアラ・ブランドホルダ１は、ＩＣカード１２を発行するイシュア２、並びに、利用者がＩＣカードを利用するための装置もしくはそれらを管理する装置である、ＰＯＳセンタ１７、ＭＭＫセンタ１９、および加盟店端末装置２１に対して、提携内容に基づいた鍵を配布するが、利用者が、パーソナルコンピュータ１４およびリーダライタ１５を用いて利用することができるサイバー店舗１６には、発行した鍵を配布せずに、自分自身に保存し、サイバー店舗１６からの要求に従って、所定のＩＣカード１２との認証処理を実行する。

【選択図】　　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社